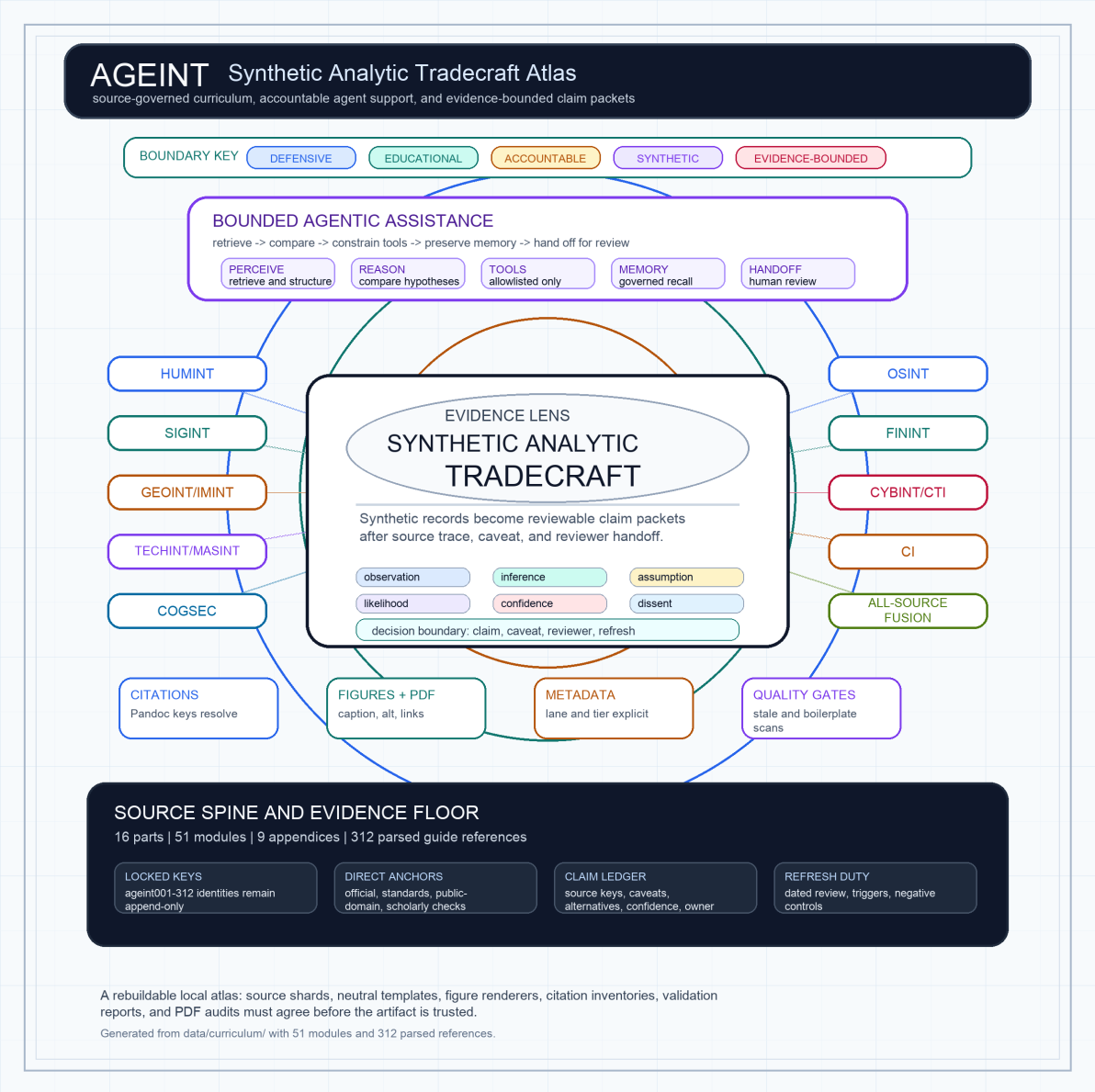
AGEINT: Agentic Intelligence

A Modular Atlas, Library, Course, Textbook, Cookbook, and Playbook for Agentic Intelligence

Daniel Ari Friedman
Active Inference Institute, FractAI
daniel@activeinference.institute
ORCID: 0000-0001-6232-9096



Edition 0.1 – 2026 DOI: 10.5281/zenodo.20732274

Publishing Information

AGEINT: Agentic Intelligence

A Modular Atlas, Library, Course, Textbook, Cookbook, and Playbook for Agentic Intelligence

Daniel Ari Friedman

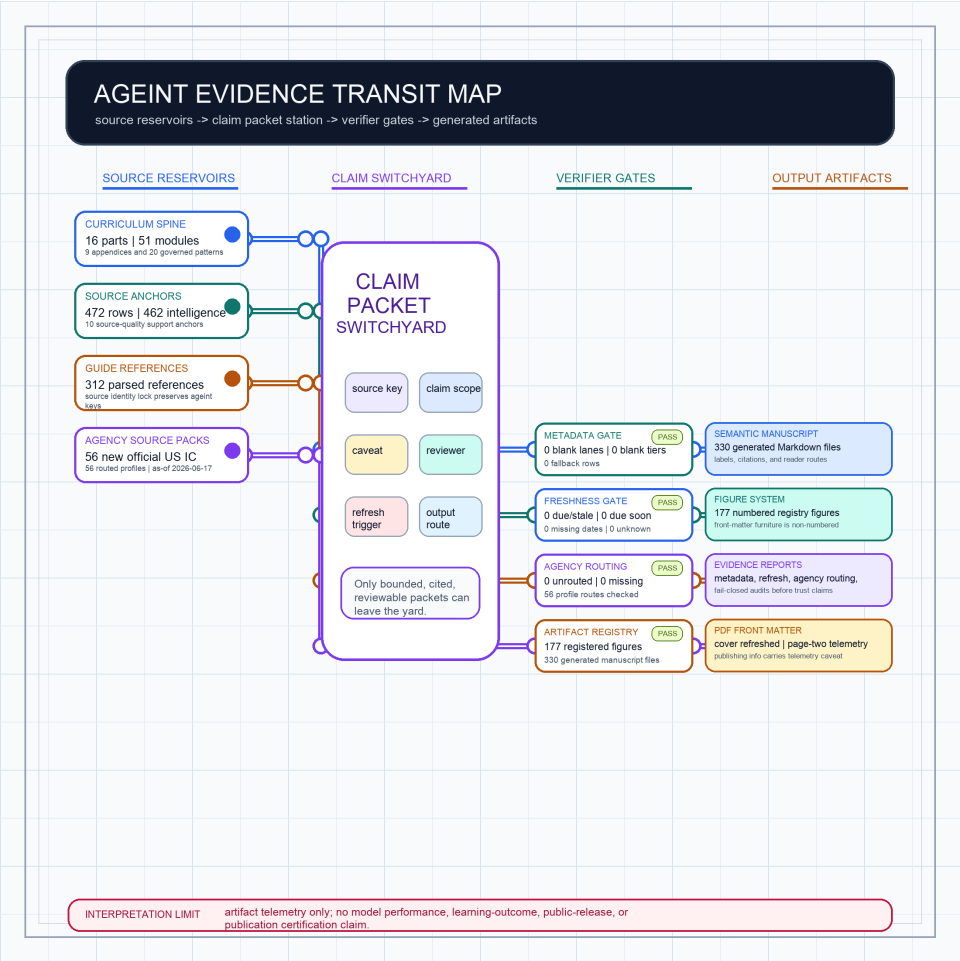
Active Inference Institute, FractAI
daniel@activeinference.institute
ORCID: 0000-0001-6232-9096

Edition 0.1 – 2026

Text license: CC BY 4.0
Source-code license: Apache-2.0

DOI: 10.5281/zenodo.20732274
docxology/AGEINT: https://github.com/docxology/AGEINT

Evidence Transit Map



Source telemetry from AGEINT curriculum counts, source metadata, source freshness, agency-source routing, figure registry, and generated manuscript files. This front-matter map is artifact telemetry only: it is not a benchmark, public-release certificate, publication claim, or learning-outcome result.

Suggested citation: Daniel Ari Friedman (2026). *AGEINT: Agentic Intelligence: A Modular Atlas, Library, Course, Textbook, Cookbook, and Playbook for Agentic Intelligence* (Edition 0.1). Active Inference Institute. https://github.com/docxology/AGEINT. https://doi.org/10.5281/zenodo.20732274.

This open textbook is generated from version-controlled Markdown, tested Python modules, programmatic figures, and rendered Mermaid diagrams. Corrections and improvements may be submitted via the source repository linked above.

Accessibility note: the compact PDF is optimized for dense print. Reader-profile builds, HTML output, and source Markdown can be generated from the same manuscript materials.

Contents

1 Abstract: Synthetic Analytic Tradecraft contract . . . 7
2 Curriculum Orientation: reader paths, evidence maps, and safety gates . . . 8
2.1 How to use this atlas: navigation path, evidence checks, and verifier handoff . . . 8
2.2 Synthetic Analytic Tradecraft thesis: synthetic fixtures, source discipline, and reviewable claims . . . 10
2.3 Reader paths: instructor, learner, reviewer, and maintainer handoffs . . . 12
2.4 Curriculum map: parts, modules, and source-backed route choices . . . 13
2.5 Runtime inventory: generated counts, anchors, and method appendices . . . 14
2.6 Related work and contribution boundary: adjacent literatures and AGEINT limits . . . 16
2.7 Analysis validation protocol: claim classes, evidence packets, and failure modes . . . 17
2.8 Consolidated glossary and index: terms, audit surfaces, and reader routing . . . 19
2.9 Intelligence research profiles: domain lanes, source roles, and profile routing . . . 20
2.10 Intelligence practice lenses: artifact expectations, safety checks, and review questions . . . 21
2.11 Research anchor atlas: curated sources, lanes, tiers, and claim scope . . . 22
2.12 Source lane map: provenance lanes, support strength, and refresh context . . . 98
2.13 Safe substitution matrix: defensive artifacts for risky inherited motifs . . . 108
2.14 Capstone workflow: phase sequence, artifacts, and reviewer gates . . . 109
2.15 Capstone model-answer exemplars: strong evidence packets and revision triggers . . . 110
2.16 Accessibility and UDL review: learner access, modality checks, and accommodation evidence . . . 111
2.17 Procurement and vendor oversight: tool governance, revocation, and vendor evidence . . . 112
2.18 HRIA and DPIA worksheet: rights impact, privacy review, and residual risk . . . 113
2.19 Data lineage registry: source identity, transformations, retention, and review . . . 114
2.20 Assessment integrity protocol: declared agent use, grading evidence, and human judgment . . . 115
2.21 Agent incident response drill: pause, revoke, preserve, recover, and debrief . . . 116
2.22 Role-based competency map: responsibilities, evidence owners, and assurance roles . . . 117
2.23 Adversarial assurance cycle: challenge rows, remediation owners, and retest evidence . . . 118
2.24 Model and dataset documentation card: intended use, provenance, caveats, and lifecycle . . . 119
2.25 Transparency and communication notice: purpose, safeguards, human review, and limits . . . 120
2.26 Records retention and audit trail: owners, retention rules, and deletion conditions . . . 121
2.27 Release and change-control gate: reuse approval, rollback, and change evidence . . . 122
2.28 Risk exception and acceptance memo: residual risk, owner approval, and review clock . . . 123
2.29 Learner support and accommodation plan: support rows, access barriers, and escalation . . . 124
2.30 Instructor question bank: prompts, evidence checks, and misconception probes . . . 125
2.31 Remediation backlog: issue owners, retest evidence, and closure boundaries . . . 126
2.32 Scholarship and governance stance: source posture, claim limits, and public-readiness boundary . . . 127
2.33 Verifier-first artifact evidence: build freshness, audits, and negative controls . . . 128
2.34 Orientation figures and course links: visual evidence, source flow, and navigation . . . 129
2.35 AGEINT pattern library: design-pattern rows, safe substitutions, and source identity . . . 155
2.36 Safety rail: accountable, synthetic, defensive, and evidence-bounded boundaries . . . 157
3 Method & Assurance Reference: claim evidence, safety gates, and refresh duties . . . 158
3.1 Source-construction and reporting protocol: discovery records and citation boundaries . . . 158
3.2 Claim calibration and statistical limits: artifact telemetry versus empirical evidence . . . 158
3.3 Method figures and course links: assurance visuals and navigation . . . 158
3.4 Capstone phase, artifact, and review-gate ladder: required handoff sequence . . . 158
3.5 Claim and evidence ledger: claim classes, evidence floors, and review duties . . . 158
3.6 Competency and mastery rubric: scoring dimensions and visible proof . . . 159
3.7 Refresh triggers and required actions: source, safety, and tool-change duties . . . 159
3.8 Safety boundary: accountable, synthetic, defensive, and evidence-bounded practice . . . 159
3.9 Mastery evidence standard: retained artifacts, reviewer challenge, and transfer . . . 159
4 FOUNDATIONS OF INTELLIGENCE TRADECRAFT . . . 160
4.1 FOUNDATIONS OF INTELLIGENCE TRADECRAFT learning spine and source route: unit purpose, module order, and evidence handoff . . . 160
5 The Nature of Intelligence . . . 165
5.1 Governed Intelligence Cycle and Dissemination Architecture frame for The Nature of Intelligence: source context, topic focus, and reader task . . . 165
5.2 Dissemination-and-Marking Control Lens path for The Nature of Intelligence: lesson cluster, safe artifact, and review . . . 167
5.3 The Nature of Intelligence assurance handoff: evidence, governance, refresh, and capstone . . . 172
6 Intelligence Community Architectures . . . 182
6.1 Analytic Tradecraft and Source Integrity frame for Intelligence Community Architectures: source context, topic focus, and reader task . . . 182
6.2 Dissemination-and-Marking Control Lens path for Intelligence Community Architectures: lesson cluster, safe artifact, and review . . . 184
6.3 Intelligence Community Architectures assurance handoff: evidence, governance, refresh, and capstone . . . 189
7 Tradecraft: Core Principles . . . 200
7.1 Governed Intelligence Cycle and Dissemination Architecture frame for Tradecraft: Core Principles: source context, topic focus, and reader task . . . 200
7.2 Structured-Judgment Lens path for Tradecraft: Core Principles: lesson cluster, safe artifact, and review . . . 202
7.3 Tradecraft: Core Principles assurance handoff: evidence, governance, refresh, and capstone . . . 207
8 HUMAN INTELLIGENCE (HUMINT) . . . 216
8.1 HUMAN INTELLIGENCE (HUMINT) learning spine and source route: unit purpose, module order, and evidence handoff . . . 216
9 Agent Recruitment . . . 220
9.1 Collection Management and Multi-INT Requirements Discipline frame for Agent Recruitment: source context, topic focus, and reader task . . . 220
9.2 Requirements-to-Evidence Lens path for Agent Recruitment: lesson cluster, safe artifact, and review . . . 222
9.3 Agent Recruitment assurance handoff: evidence, governance, refresh, and capstone . . . 227
10 Agent Handling and Management . . . 237
10.1 Collection Management and Multi-INT Requirements Discipline frame for Agent Handling and Management: source context, topic focus, and reader task . . . 237
10.2 Requirements-to-Evidence Lens path for Agent Handling and Management: lesson cluster, safe artifact, and review . . . 239
10.3 Agent Handling and Management assurance handoff: evidence, governance, refresh, and capstone . . . 245

11 Source Protection and CI Integration . . . 256
11.1 Collection Management and Multi-INT Requirements Discipline frame for Source Protection and CI Integration: source context, topic focus, and reader task . . . 256
11.2 Requirements-to-Evidence Lens path for Source Protection and CI Integration: lesson cluster, safe artifact, and review . . . 258
11.3 Source Protection and CI Integration assurance handoff: evidence, governance, refresh, and capstone . . . 262
12 SIGNALS INTELLIGENCE (SIGINT) . . . 271
12.1 SIGNALS INTELLIGENCE (SIGINT) learning spine and source route: unit purpose, module order, and evidence handoff . . . 271
13 SIGINT Fundamentals . . . 274
13.1 Collection Management and Multi-INT Requirements Discipline frame for SIGINT Fundamentals: source context, topic focus, and reader task . . . 274
13.2 Requirements-to-Evidence Lens path for SIGINT Fundamentals: lesson cluster, safe artifact, and review . . . 276
13.3 SIGINT Fundamentals assurance handoff: evidence, governance, refresh, and capstone . . . 280
14 Modern SIGINT and Cryptography . . . 289
14.1 Collection Management and Multi-INT Requirements Discipline frame for Modern SIGINT and Cryptography: source context, topic focus, and reader task . . . 289
14.2 Requirements-to-Evidence Lens path for Modern SIGINT and Cryptography: lesson cluster, safe artifact, and review . . . 291
14.3 Modern SIGINT and Cryptography assurance handoff: evidence, governance, refresh, and capstone . . . 296
15 OPEN SOURCE INTELLIGENCE (OSINT) . . . 307
15.1 OPEN SOURCE INTELLIGENCE (OSINT) learning spine and source route: unit purpose, module order, and evidence handoff . . . 307
16 OSINT Foundations . . . 311
16.1 Open-Source and Geospatial Intelligence Integrity frame for OSINT Foundations: source context, topic focus, and reader task . . . 311
16.2 Requirements-to-Evidence Lens path for OSINT Foundations: lesson cluster, safe artifact, and review . . . 313
16.3 OSINT Foundations assurance handoff: evidence, governance, refresh, and capstone . . . 317
17 OSINT Techniques and Tools . . . 325
17.1 Open-Source and Geospatial Intelligence Integrity frame for OSINT Techniques and Tools: source context, topic focus, and reader task . . . 325
17.2 Requirements-to-Evidence Lens path for OSINT Techniques and Tools: lesson cluster, safe artifact, and review . . . 327
17.3 OSINT Techniques and Tools assurance handoff: evidence, governance, refresh, and capstone . . . 332
18 GEOINT and Imagery Intelligence . . . 342
18.1 Open-Source and Geospatial Intelligence Integrity frame for GEOINT and Imagery Intelligence: source context, topic focus, and reader task . . . 342
18.2 Requirements-to-Evidence Lens path for GEOINT and Imagery Intelligence: lesson cluster, safe artifact, and review . . . 346
18.3 GEOINT and Imagery Intelligence assurance handoff: evidence, governance, refresh, and capstone . . . 351
19 TECHNICAL INTELLIGENCE AND CYBER OPERATIONS . . . 361
19.1 TECHNICAL INTELLIGENCE AND CYBER OPERATIONS learning spine and source route: unit purpose, module order, and evidence handoff . . . 361
20 Cyber Intelligence Fundamentals . . . 365
20.1 Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense frame for Cyber Intelligence Fundamentals: source context, topic focus, and reader task . . . 365
20.2 Defensive Cyber-Intelligence Lens path for Cyber Intelligence Fundamentals: lesson cluster, safe artifact, and review . . . 367
20.3 Cyber Intelligence Fundamentals assurance handoff: evidence, governance, refresh, and capstone . . . 373
21 Advanced Persistent Threats (APTs) . . . 385
21.1 Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense frame for Advanced Persistent Threats (APTs): source context, topic focus, and reader task . . . 385
21.2 Defensive Cyber-Intelligence Lens path for Advanced Persistent Threats (APTs): lesson cluster, safe artifact, and review . . . 387
21.3 Advanced Persistent Threats (APTs) assurance handoff: evidence, governance, refresh, and capstone . . . 391
22 Supply Chain Intelligence Attacks . . . 401
22.1 Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense frame for Supply Chain Intelligence Attacks: source context, topic focus, and reader task . . . 401
22.2 Software-Supply-Chain Assurance Lens path for Supply Chain Intelligence Attacks: lesson cluster, safe artifact, and review . . . 403
22.3 Supply Chain Intelligence Attacks assurance handoff: evidence, governance, refresh, and capstone . . . 408
23 Electronic and Emanations Intelligence . . . 419
23.1 Collection Management and Multi-INT Requirements Discipline frame for Electronic and Emanations Intelligence: source context, topic focus, and reader task . . . 419
23.2 Dissemination-and-Marking Control Lens path for Electronic and Emanations Intelligence: lesson cluster, safe artifact, and review . . . 421
23.3 Electronic and Emanations Intelligence assurance handoff: evidence, governance, refresh, and capstone . . . 425
24 IMAGERY AND FINANCIAL INTELLIGENCE . . . 435
24.1 IMAGERY AND FINANCIAL INTELLIGENCE learning spine and source route: unit purpose, module order, and evidence handoff . . . 435
25 Imagery Intelligence (IMINT) . . . 438
25.1 Open-Source and Geospatial Intelligence Integrity frame for Imagery Intelligence (IMINT): source context, topic focus, and reader task . . . 438
25.2 Requirements-to-Evidence Lens path for Imagery Intelligence (IMINT): lesson cluster, safe artifact, and review . . . 442
25.3 Imagery Intelligence (IMINT) assurance handoff: evidence, governance, refresh, and capstone . . . 446
26 Financial Intelligence (FININT) . . . 455
26.1 Financial Intelligence and Economic-Security Due Diligence frame for Financial Intelligence (FININT): source context, topic focus, and reader task . . . 455
26.2 Economic-Security Due-Diligence Lens path for Financial Intelligence (FININT): lesson cluster, safe artifact, and review . . . 457
26.3 Financial Intelligence (FININT) assurance handoff: evidence, governance, refresh, and capstone . . . 462
27 PSYCHOLOGICAL OPERATIONS AND INFLUENCE . . . 472
27.1 PSYCHOLOGICAL OPERATIONS AND INFLUENCE learning spine and source route: unit purpose, module order, and evidence handoff . . . 472
28 PSYOP and MISO Doctrine . . . 476
28.1 Cognitive Security and Influence Resilience frame for PSYOP and MISO Doctrine: source context, topic focus, and reader task . . . 476
28.2 Cognitive-Resilience Lens path for PSYOP and MISO Doctrine: lesson cluster, safe artifact, and review . . . 478
28.3 PSYOP and MISO Doctrine assurance handoff: evidence, governance, refresh, and capstone . . . 482
29 Active Measures and Disinformation . . . 492
29.1 Cognitive Security and Influence Resilience frame for Active Measures and Disinformation: source context, topic focus, and reader task . . . 492
29.2 Cognitive-Resilience Lens path for Active Measures and Disinformation: lesson cluster, safe artifact, and review . . . 494

29.3 Active Measures and Disinformation assurance handoff: evidence, governance, refresh, and capstone . . . 499
30 Social Engineering . . . 510
30.1 Cognitive Security and Influence Resilience frame for Social Engineering: source context, topic focus, and reader task . . . 510
30.2 Cognitive-Resilience Lens path for Social Engineering: lesson cluster, safe artifact, and review . . . 512
30.3 Social Engineering assurance handoff: evidence, governance, refresh, and capstone . . . 516
31 Information Warfare and Cognitive Security . . . 525
31.1 Cognitive Security and Influence Resilience frame for Information Warfare and Cognitive Security: source context, topic focus, and reader task . . . 525
31.2 Cognitive-Resilience Lens path for Information Warfare and Cognitive Security: lesson cluster, safe artifact, and review . . . 527
31.3 Information Warfare and Cognitive Security assurance handoff: evidence, governance, refresh, and capstone . . . 531
32 COUNTERINTELLIGENCE . . . 541
32.1 COUNTERINTELLIGENCE learning spine and source route: unit purpose, module order, and evidence handoff . . . 541
33 Counterintelligence Fundamentals . . . 544
33.1 Counterintelligence and Source-Integrity Defense frame for Counterintelligence Fundamentals: source context, topic focus, and reader task . . . 544
33.2 Structured-Judgment Lens path for Counterintelligence Fundamentals: lesson cluster, safe artifact, and review . . . 546
33.3 Counterintelligence Fundamentals assurance handoff: evidence, governance, refresh, and capstone . . . 551
34 Counterintelligence Against Non-State Actors . . . 561
34.1 Counterintelligence and Source-Integrity Defense frame for Counterintelligence Against Non-State Actors: source context, topic focus, and reader task . . . 561
34.2 Structured-Judgment Lens path for Counterintelligence Against Non-State Actors: lesson cluster, safe artifact, and review . . . 563
34.3 Counterintelligence Against Non-State Actors assurance handoff: evidence, governance, refresh, and capstone . . . 567
35 GRAY ZONE, HYBRID WARFARE, AND NON-STATE ACTORS . . . 576
35.1 GRAY ZONE, HYBRID WARFARE, AND NON-STATE ACTORS learning spine and source route: unit purpose, module order, and evidence handoff . . . 576
36 Gray Zone Warfare . . . 580
36.1 Counterintelligence and Source-Integrity Defense frame for Gray Zone Warfare: source context, topic focus, and reader task . . . 580
36.2 Dissemination-and-Marking Control Lens path for Gray Zone Warfare: lesson cluster, safe artifact, and review . . . 582
36.3 Gray Zone Warfare assurance handoff: evidence, governance, refresh, and capstone . . . 586
37 Non-State Actor Intelligence . . . 596
37.1 Counterintelligence and Source-Integrity Defense frame for Non-State Actor Intelligence: source context, topic focus, and reader task . . . 596
37.2 Dissemination-and-Marking Control Lens path for Non-State Actor Intelligence: lesson cluster, safe artifact, and review . . . 598
37.3 Non-State Actor Intelligence assurance handoff: evidence, governance, refresh, and capstone . . . 602
38 Irregular Warfare and Special Operations . . . 612
38.1 Counterintelligence and Source-Integrity Defense frame for Irregular Warfare and Special Operations: source context, topic focus, and reader task . . . 612
38.2 Dissemination-and-Marking Control Lens path for Irregular Warfare and Special Operations: lesson cluster, safe artifact, and review . . . 614
38.3 Irregular Warfare and Special Operations assurance handoff: evidence, governance, refresh, and capstone . . . 619
39 HISTORICAL INTELLIGENCE SERVICES . . . 630
39.1 HISTORICAL INTELLIGENCE SERVICES learning spine and source route: unit purpose, module order, and evidence handoff 630
40 Soviet and Russian Intelligence . . . 634
40.1 Historical and Declassified Intelligence Services frame for Soviet and Russian Intelligence: source context, topic focus, and reader task . . . 634
40.2 Historical Case-Translation Lens path for Soviet and Russian Intelligence: lesson cluster, safe artifact, and review . . . 636
40.3 Soviet and Russian Intelligence assurance handoff: evidence, governance, refresh, and capstone . . . 642
41 American Intelligence History . . . 654
41.1 Historical and Declassified Intelligence Services frame for American Intelligence History: source context, topic focus, and reader task . . . 654
41.2 Historical Case-Translation Lens path for American Intelligence History: lesson cluster, safe artifact, and review . . . 656
41.3 American Intelligence History assurance handoff: evidence, governance, refresh, and capstone . . . 663
42 British and Allied Intelligence . . . 676
42.1 Historical and Declassified Intelligence Services frame for British and Allied Intelligence: source context, topic focus, and reader task . . . 676
42.2 Historical Case-Translation Lens path for British and Allied Intelligence: lesson cluster, safe artifact, and review . . . 678
42.3 British and Allied Intelligence assurance handoff: evidence, governance, refresh, and capstone . . . 681
43 Israeli and Continental Services . . . 691
43.1 Historical and Declassified Intelligence Services frame for Israeli and Continental Services: source context, topic focus, and reader task . . . 691
43.2 Historical Case-Translation Lens path for Israeli and Continental Services: lesson cluster, safe artifact, and review . . . 693
43.3 Israeli and Continental Services assurance handoff: evidence, governance, refresh, and capstone . . . 697
44 AGEINT — AGENTIC INTELLIGENCE . . . 706
44.1 AGEINT — AGENTIC INTELLIGENCE learning spine and source route: unit purpose, module order, and evidence handoff 706
45 Foundations of AGEINT . . . 711
45.1 Agentic AI Governance and Tool Security frame for Foundations of AGEINT: source context, topic focus, and reader task . . . 711
45.2 Agentic Tool-Governance Lens path for Foundations of AGEINT: lesson cluster, safe artifact, and review . . . 713
45.3 Foundations of AGEINT assurance handoff: evidence, governance, refresh, and capstone . . . 719
46 AGEINT Design Patterns and Archetypes . . . 730
46.1 Agentic AI Governance and Tool Security frame for AGEINT Design Patterns and Archetypes: source context, topic focus, and reader task . . . 730
46.2 Agentic Tool-Governance Lens path for AGEINT Design Patterns and Archetypes: lesson cluster, safe artifact, and review . . . 733
46.3 AGEINT Design Patterns and Archetypes assurance handoff: evidence, governance, refresh, and capstone . . . 766
47 AGEINT Frameworks and Infrastructure . . . 789
47.1 Agentic AI Governance and Tool Security frame for AGEINT Frameworks and Infrastructure: source context, topic focus, and reader task . . . 789
47.2 Agentic Tool-Governance Lens path for AGEINT Frameworks and Infrastructure: lesson cluster, safe artifact, and review . . . 791
47.3 AGEINT Frameworks and Infrastructure assurance handoff: evidence, governance, refresh, and capstone . . . 802
48 AGEINT Security and Adversarial Considerations . . . 816
48.1 Agentic AI Governance and Tool Security frame for AGEINT Security and Adversarial Considerations: source context, topic focus, and reader task . . . 816

48.2 Defensive Cyber-Intelligence Lens path for AGEINT Security and Adversarial Considerations: lesson cluster, safe artifact, and review . . . 829
48.3 AGEINT Security and Adversarial Considerations assurance handoff: evidence, governance, refresh, and capstone . . . 838
49 Active Inference and AGEINT . . . 852
49.1 Active-Inference Theory and Governed Agent Analogy frame for Active Inference and AGEINT: source context, topic focus, and reader task . . . 852
49.2 Active-Inference Boundary Lens path for Active Inference and AGEINT: lesson cluster, safe artifact, and review . . . 855
49.3 Active Inference and AGEINT assurance handoff: evidence, governance, refresh, and capstone . . . 859
50 AGEINT Python Code Library . . . 870
50.1 Agentic AI Governance and Tool Security frame for AGEINT Python Code Library: source context, topic focus, and reader task . . . 870
50.2 Agentic Tool-Governance Lens path for AGEINT Python Code Library: lesson cluster, safe artifact, and review . . . 872
50.3 AGEINT Python Code Library assurance handoff: evidence, governance, refresh, and capstone . . . 877
51 COGNITIVE SECURITY . . . 888
51.1 COGNITIVE SECURITY learning spine and source route: unit purpose, module order, and evidence handoff . . . 888
51.2 How adversaries target cognition . . . 888
52 Cognitive Security: Foundations and Definitions . . . 894
52.1 Cognitive Security and Influence Resilience frame for Cognitive Security: Foundations and Definitions: source context, topic focus, and reader task . . . 894
52.2 Cognitive-Resilience Lens path for Cognitive Security: Foundations and Definitions: lesson cluster, safe artifact, and review . . . 896
52.3 Cognitive Security: Foundations and Definitions assurance handoff: evidence, governance, refresh, and capstone . . . 904
53 Neurocognitive Mechanisms of Cognitive Security . . . 917
53.1 Cognitive Security and Influence Resilience frame for Neurocognitive Mechanisms of Cognitive Security: source context, topic focus, and reader task . . . 917
53.2 Cognitive-Resilience Lens path for Neurocognitive Mechanisms of Cognitive Security: lesson cluster, safe artifact, and review 919
53.3 Neurocognitive Mechanisms of Cognitive Security assurance handoff: evidence, governance, refresh, and capstone . . . 925
54 Psychological Inoculation and Prebunking . . . 935
54.1 Cognitive Security and Influence Resilience frame for Psychological Inoculation and Prebunking: source context, topic focus, and reader task . . . 935
54.2 Cognitive-Resilience Lens path for Psychological Inoculation and Prebunking: lesson cluster, safe artifact, and review . . . 938
54.3 Psychological Inoculation and Prebunking assurance handoff: evidence, governance, refresh, and capstone . . . 944
55 Cognitive Security Operations . . . 955
55.1 Cognitive Security and Influence Resilience frame for Cognitive Security Operations: source context, topic focus, and reader task . . . 955
55.2 Cognitive-Resilience Lens path for Cognitive Security Operations: lesson cluster, safe artifact, and review . . . 957
55.3 Cognitive Security Operations assurance handoff: evidence, governance, refresh, and capstone . . . 962
56 EPISTEMIC RIGOR AND ANALYTIC TRADECRAFT . . . 972
56.1 EPISTEMIC RIGOR AND ANALYTIC TRADECRAFT learning spine and source route: unit purpose, module order, and evidence handoff . . . 972
56.2 The unified epistemic coherence stack . . . 972
56.3 From reliability theory to AI governance . . . 972
57 Structured Analytic Techniques (SATs) . . . 978
57.1 Analytic Tradecraft and Source Integrity frame for Structured Analytic Techniques (SATs): source context, topic focus, and reader task . . . 978
57.2 Structured-Judgment Lens path for Structured Analytic Techniques (SATs): lesson cluster, safe artifact, and review . . . 984
57.3 Structured Analytic Techniques (SATs) assurance handoff: evidence, governance, refresh, and capstone . . . 991
58 Advanced Analysis Methods . . . 1003
58.1 Analytic Tradecraft and Source Integrity frame for Advanced Analysis Methods: source context, topic focus, and reader task 1003
58.2 Structured-Judgment Lens path for Advanced Analysis Methods: lesson cluster, safe artifact, and review . . . 1008
58.3 Advanced Analysis Methods assurance handoff: evidence, governance, refresh, and capstone . . . 1012
59 PRODUCTIVITY INTELLIGENCE AND COGNITIVE PERFORMANCE . . . 1021
59.1 PRODUCTIVITY INTELLIGENCE AND COGNITIVE PERFORMANCE learning spine and source route: unit purpose, module order, and evidence handoff . . . 1021
60 The Intelligent Operator as Cognitive Athlete . . . 1025
60.1 Operator Productivity and Cognitive Performance frame for The Intelligent Operator as Cognitive Athlete: source context, topic focus, and reader task . . . 1025
60.2 Operator-Workload Hygiene Lens path for The Intelligent Operator as Cognitive Athlete: lesson cluster, safe artifact, and review . . . 1027
60.3 The Intelligent Operator as Cognitive Athlete assurance handoff: evidence, governance, refresh, and capstone . . . 1037
61 Information Architecture for Intelligence Work . . . 1052
61.1 Governed Intelligence Cycle and Dissemination Architecture frame for Information Architecture for Intelligence Work: source context, topic focus, and reader task . . . 1052
61.2 Dissemination-and-Marking Control Lens path for Information Architecture for Intelligence Work: lesson cluster, safe artifact, and review . . . 1055
61.3 Information Architecture for Intelligence Work assurance handoff: evidence, governance, refresh, and capstone . . . 1060
62 INDUSTRIAL AND CYBER-PHYSICAL INTELLIGENCE . . . 1071
62.1 INDUSTRIAL AND CYBER-PHYSICAL INTELLIGENCE learning spine and source route: unit purpose, module order, and evidence handoff . . . 1071
63 Industrial Control Systems (ICS) and Operational Technology . . . 1075
63.1 ICS/OT Cyber-Physical Defense and Tabletop Readiness frame for Industrial Control Systems (ICS) and Operational Technology: source context, topic focus, and reader task . . . 1075
63.2 Cyber-Physical Readiness Lens path for Industrial Control Systems (ICS) and Operational Technology: lesson cluster, safe artifact, and review . . . 1078
63.3 Industrial Control Systems (ICS) and Operational Technology assurance handoff: evidence, governance, refresh, and capstone 1083
64 MITRE ATT&CK for ICS . . . 1093
64.1 ICS/OT Cyber-Physical Defense and Tabletop Readiness frame for MITRE ATT&CK for ICS: source context, topic focus, and reader task . . . 1093
64.2 Cyber-Physical Readiness Lens path for MITRE ATT&CK for ICS: lesson cluster, safe artifact, and review . . . 1095
64.3 MITRE ATT&CK for ICS assurance handoff: evidence, governance, refresh, and capstone . . . 1102
65 Historical ICS Cyber Incidents: Intelligence Analysis . . . 1113

65.1 ICS/OT Cyber-Physical Defense and Tabletop Readiness frame for Historical ICS Cyber Incidents: Intelligence Analysis: source context, topic focus, and reader task . . . 1113
65.2 Cyber-Physical Readiness Lens path for Historical ICS Cyber Incidents: Intelligence Analysis: lesson cluster, safe artifact, and review . . . 1115
65.3 Historical ICS Cyber Incidents: Intelligence Analysis assurance handoff: evidence, governance, refresh, and capstone . . . 1120
66 Threat Intelligence Sharing for Critical Infrastructure . . . 1130
66.1 ICS/OT Cyber-Physical Defense and Tabletop Readiness frame for Threat Intelligence Sharing for Critical Infrastructure: source context, topic focus, and reader task . . . 1130
66.2 Cyber-Physical Readiness Lens path for Threat Intelligence Sharing for Critical Infrastructure: lesson cluster, safe artifact, and review . . . 1132
66.3 Threat Intelligence Sharing for Critical Infrastructure assurance handoff: evidence, governance, refresh, and capstone . . . 1136
67 AGEINT Applied to ICS and Cyber-Physical Intelligence . . . 1146
67.1 ICS/OT Cyber-Physical Defense and Tabletop Readiness frame for AGEINT Applied to ICS and Cyber-Physical Intelligence: source context, topic focus, and reader task . . . 1146
67.2 Cyber-Physical Readiness Lens path for AGEINT Applied to ICS and Cyber-Physical Intelligence: lesson cluster, safe artifact, and review . . . 1149
67.3 AGEINT Applied to ICS and Cyber-Physical Intelligence assurance handoff: evidence, governance, refresh, and capstone . . . 1153
68 LEGAL, ETHICAL, AND OVERSIGHT FRAMEWORKS . . . 1163
68.1 LEGAL, ETHICAL, AND OVERSIGHT FRAMEWORKS learning spine and source route: unit purpose, module order, and evidence handoff . . . 1163
69 Legal Authorities and Constraints . . . 1166
69.1 Legal, Ethical, and Oversight Architecture frame for Legal Authorities and Constraints: source context, topic focus, and reader task . . . 1166
69.2 Oversight-and-Rights Lens path for Legal Authorities and Constraints: lesson cluster, safe artifact, and review . . . 1168
69.3 Legal Authorities and Constraints assurance handoff: evidence, governance, refresh, and capstone . . . 1172
70 Ethics of Intelligence and Cognitive Security . . . 1181
70.1 Legal, Ethical, and Oversight Architecture frame for Ethics of Intelligence and Cognitive Security: source context, topic focus, and reader task . . . 1181
70.2 Oversight-and-Rights Lens path for Ethics of Intelligence and Cognitive Security: lesson cluster, safe artifact, and review . . . 1183
70.3 Ethics of Intelligence and Cognitive Security assurance handoff: evidence, governance, refresh, and capstone . . . 1187
71 Python OSINT Library . . . 1196
71.1 Python OSINT Library workbook scope: purpose, safety envelope, and reuse decision . . . 1196
72 LangChain/LangGraph AGEINT Patterns . . . 1201
72.1 LangChain/LangGraph AGEINT Patterns workbook scope: purpose, safety envelope, and reuse decision . . . 1201
73 CrewAI Multi-Agent Operations . . . 1206
73.1 CrewAI Multi-Agent Operations workbook scope: purpose, safety envelope, and reuse decision . . . 1206
74 AutoGen and MCP Patterns . . . 1211
74.1 AutoGen and MCP Patterns workbook scope: purpose, safety envelope, and reuse decision . . . 1211
74.2 MCP and AutoGen source boundary . . . 1214
75 Cryptographic Methods . . . 1217
75.1 Cryptographic Methods workbook scope: purpose, safety envelope, and reuse decision . . . 1217
75.2 Cryptographic standards boundary . . . 1220
76 ATT&CK and Kill Chain Mapping Templates . . . 1222
76.1 ATT&CK and Kill Chain Mapping Templates workbook scope: purpose, safety envelope, and reuse decision . . . 1222
77 Cognitive Security and Inoculation Methods . . . 1227
77.1 Cognitive Security and Inoculation Methods workbook scope: purpose, safety envelope, and reuse decision . . . 1227
77.2 Cognitive degradation as a staged cascade . . . 1230
77.3 The decoherence-degradation isomorphism . . . 1230
78 Source Verification and Claim Ledger Workbook . . . 1233
78.1 Source Verification and Claim Ledger Workbook workbook scope: purpose, safety envelope, and reuse decision . . . 1233
78.2 Source verification workflow . . . 1236
78.3 Source refresh evidence . . . 1245
78.4 HRIA/DPIA evidence bridge . . . 1246
79 Instructor Capstone, Rubric, and Red-Team Review Pack . . . 1254
79.1 Instructor Capstone, Rubric, and Red-Team Review Pack workbook scope: purpose, safety envelope, and reuse decision . . . 1254
79.2 Instructor capstone workflow . . . 1257
79.3 Safe artifact rows . . . 1257
79.4 Assessment lifecycle evidence . . . 1257
79.5 Adversarial review evidence . . . 1257
80 Bibliography Atlas: source keys, refresh evidence, and citation workflow . . . 1268
80.1 Bibliography atlas navigation figures and source links: visual route through citation evidence . . . 1268
80.2 Current-source additions and refreshes: newly checked anchors and changed caveats . . . 1275
80.3 Source refresh ledger: cadence, checked dates, and due-status evidence . . . 1308
80.4 Citation workflow and source-section coverage . . . 1375
80.5 Add or extend a citation: preserve identity and record metadata . . . 1376
80.6 Add or extend a citation: preserve identity and record metadata (continued 2) . . . 1411
80.7 Bibliography atlas rows: guide keys, curated anchors, and support-source roles . . . 1432
80.8 Bibliography atlas rows: guide keys, curated anchors, and support-source roles {#sec:bibliography-rows} (continued 2) . . . 1693
References . . . 1791

1 Abstract: Synthetic Analytic Tradecraft contract

AGEINT, or Agentic Intelligence, is a local curriculum-and-assurance atlas for teaching bounded AI-agent support inside intelligence education by making the machinery of Synthetic Analytic Tradecraft visible on the page. It converts SIST Guide TOC and Bibliography into **16 parts**, **51 modules**, **9 methods appendices**, **20 named AGEINT patterns**, and **312 parsed source-guide references** without renumbering inherited source identities, then asks the reader to inspect the same things an instructor or assurance reviewer would inspect: the part map that frames the domain, the module overview that names the learner task, the source spine that separates official, standards, scholarly, public-domain, practitioner, vendor, and provenance-only support while separating source quality from narrative fluency, the evidence packet that a student would retain, the reviewer challenge that should break a weak claim, and the validators that prevent a polished artifact from masquerading as a verified one. A learner does not enter through a slogan. The learner opens a module, sees which authority and source keys are allowed to carry the claim, reads a textbook primer that distinguishes observation from inference, confidence from probability, and source quality from fluency, works through a synthetic practice studio using classroom records, public declassified examples, owned-lab logs, toy datasets, rendered figures, or tabletop incidents, and then produces a bounded artifact with caveats, assumptions, alternatives, excluded actions, human review, rollback evidence, and refresh triggers written into the record before reuse. The method contract in Figure 19 shows that flow as a claim-to-evidence pathway rather than as an aspirational ethics statement: authority must be named before the task begins, source support must be traceable before a claim is promoted, unsafe action must be replaced by safe substitution, and agentic assistance must remain a drafting, retrieval, comparison, simulation, critique, or audit aid whose output is never treated as self-authenticating [of the Director of National Intelligence, 2015] [Agency, 2009] [Jr., 2007]. AGEINT remains synthetic in its fixtures, not in its standards: the word synthetic is therefore a control, not a downgrade. AGEINT keeps the fixture safe while keeping the standard difficult: HUMINT, SIGINT, OSINT, GEOINT and IMINT, FININT, counterintelligence, cyber threat intelligence, cognitive security, agent orchestration, active inference, source verification, public-sector governance, privacy review, and industrial-control-system defense can be discussed because the student is not handed live targets, evasion recipes, exploit instructions, manipulation playbooks, covert-action procedures, or unsafe cyber-physical steps. When a source topic could invite misuse, the module turns the risky motif into a provenance card, detection-coverage note, rights-impact worksheet, model or dataset card, source-refresh memo, release gate, risk-exception log, remediation backlog, or debrief protocol, and the exercise fails if it cannot show where authority, data boundary, tool permission, uncertainty, and review enter the workflow. The source layer is intentionally conservative: Perplexity and similar discovery tools may suggest candidates, but the manuscript cites verified official, standards, public-domain, or scholarly anchors encoded in the source corpus and rebuilt into BibTeX; Practitioner, vendor, and blog sources inherited through the source guide, plus social or other guide-inherited rows, can preserve provenance context without becoming foundational support for governance, rights, safety, empirical, statistical, or performance claims unless a stronger verified source bears the specific point. The same source posture is visible in the counts: 10 source-quality anchors cover the governing standards and assurance spine, while 462 curated intelligence research anchors span the domain lanes that route claim-bearing prose to direct evidence rather than decorative citations. A strong AGEINT artifact is therefore not an uninspected essay. It is an evidence packet that names the question, allowed inputs, excluded actions, source keys, claim type, caveats, competing explanations, confidence basis, prompt or run card, tool allowlist, data boundary, stop condition, reviewer challenge, safety boundary, refresh trigger, and human disposition. It also contains negative controls: stale citations that should be caught, weak-source-only claims that should be downgraded, figure positions or colors that should not be mistaken for quantitative evidence, overbroad statistical language that should fail, and operational substitutions that should halt until an instructor or reviewer approves a safer artifact. A reviewer can trace a finished packet in both directions: from a polished sentence back to the claim class, source family, cited anchor, caveat, and source-refresh duty, or from a source row forward to the modules, figures, tables, and exercises that rely on it. A student can see why a governance claim needs law, policy, standard, or official guidance support; why a cyber or industrial-control-system scenario must remain defensive and synthetic; why a social or cognitive-security lesson must become resilience education rather than persuasion practice; why a vendor or practitioner note can motivate a question but cannot by itself carry a public-rights or safety assertion; why a figure caption must say whether arrows are explanatory or quantitative; and why a model-generated draft is only useful after it has been constrained by authority, reviewed by a person, and attached to evidence that another person can contest. The early orientation pages, part maps, chapter landmarks, appendices, bibliography atlas, source-lane map, and generated reports are designed to make that trace visible instead of leaving it to instructor memory. They show the learner what to keep: the source keys behind each claim, the reason a safer substitute was chosen, the assumption that would change the answer, the dissent that should not be smoothed away, the review note that records who accepted residual risk, the rollback path if a source or permission changes, and the refresh trigger that turns a current claim back into a review item. They also show what the curriculum refuses to keep: unverifiable authority theater, live-target instructions, metric-looking diagrams without units or denominators, statistical decorations without empirical design, citation clusters that do not bear the sentence they decorate, and agent outputs whose provenance cannot be reconstructed. The technical build is part of that scholarship. Curriculum shards generate semantic manuscript files; cross-references use label-backed section and figure links, and display equations are typeset from source for reproducible math; citations route through Pandoc keys; figures are registry-backed PNG assets with captions, alt text, long descriptions, provenance, hashes, and visual-semantics metadata; source anchors carry explicit lane and tier fields; claim calibration audits high-risk empirical, statistical, governance, safety, visualization, artifact-readiness, and formalism language; scholarship and source-metadata reports expose review warnings instead of hiding them; PDF audits check stale output, URI targets, file actions, and banned filler language. The analysis-validation matrix in Figure 20 names which claim classes require empirical evidence, direct source-family support, negative controls, figure semantics, or rendered-artifact checks before they can be treated as ready, and that matrix is a boundary on what the manuscript can honestly say. AGEINT is not a benchmark and does not claim to measure AGEINT performance, model capability, analyst replacement, learning outcomes, operational effectiveness, public-sector impact, statistical significance, or safety performance; page counts, citation counts, figure counts, validator passes, and link audits are artifact telemetry, not empirical outcome evidence. Its strongest claim is methodological and inspectable: agentic assistance can be taught inside intelligence education when every reuse path is forced through authority, source support, safe substitution, evidence packet, negative controls, human review, rollback, and refresh triggers, and when the safest failure mode is to stop, document the unresolved condition, and ask for review. The resulting work should be read as a Synthetic Analytic Tradecraft atlas, not as a public-release certificate or a disguised operational manual: the reader can see the source key behind a sentence, the caveat behind a confidence statement, the assumption behind a scenario, the blocked use behind a tempting automation, the challenge behind a polished answer, the caption that limits a visual, the validator that rejects an overclaim, and the refresh duty that keeps current-source prose from becoming stale authority.

2 Curriculum Orientation: reader paths, evidence maps, and safety gates

AGEINT (Agentic Intelligence) is a curriculum-and-assurance atlas for teaching how AI agents can *assist* intelligence analysis without ever being trusted to run it unsupervised. It is written for three readers: an **instructor** assembling a defensible course, a **learner** building analytic habits on safe practice material, and an **assurance reviewer** checking that every claim can be traced back to a real source. Nothing here is operational — every exercise uses synthetic or public material, and every claim is built to be challenged rather than believed.

Read it as a map, not a textbook to read front to back: Section 2.4 lets you choose a domain part, Section 2.3 gives each reader a fast path, and Section 2.36 states what the atlas refuses to teach.

> **For maintainers.** This page is generated. The source templates under `manuscript/templates/` keep guide-derived values — titles, labels, counts, source spines, semantic paths, and bibliography rows — as neutral tokens; the build resolves them from `data/curriculum/` into the rendered manuscript in `output/manuscript/`. Edit the template, not the rendered output.

The rest of this orientation is a toolkit for navigating that map; the next section shows the exact path.

2.1 How to use this atlas: navigation path, evidence checks, and verifier handoff

Read AGEINT as a navigable curriculum-and-assurance atlas rather than a linear textbook or empirical evaluation report. Start with Section 2.4 and Figure 5 to choose the part, open the linked part introduction to see the module sequence, then use each chapter overview for the figures, source lane, and assessment artifact that matter for the current decision. Keep Section 80 open when checking a claim, because it preserves source identity, provenance type, source tier, and refresh context in one place.

Use the first pages as signposts, not as a preface to skip. The handoff is intentionally explicit and always moves in the same direction:

domain part -> module overview -> practice studio -> evidence contract -> governance boundary -> assessment route -> bibliography/source lane -> verifier reports.

Work the table below in order: orient, then match each claim to its evidence, then verify before trusting anything.

Step	Where to go	Why this step matters
Start here	Section 2.4, Section 2.2, and Section 2.3	Choose a domain part, name the Synthetic Analytic Tradecraft contract, and decide which reader path governs the next move.
Then check	Section 2.7, Section 2.12, and Section 80	Match the claim class to evidence, lane, citation identity, and refresh duty before treating prose or figures as support.
Before you trust	Section 2.13, Section 2.34, and Section 3	Confirm risky motifs were converted to bounded artifacts, figures carry their limits, and verifier reports agree with the rendered manuscript.
Govern and assure	Section 2.18, Section 2.23, Section 2.24, and Section 2.26	Bind rights impact, red-team challenge, documentation provenance, and retention duty to each reusable artifact before it leaves the course.

Claim classes are separated at source-selection time. Governance claims, technical and theoretical claims, empirical capability claims, and source-construction claims each need a matching evidence type; the shared method reference records the PRISMA-S-inspired source-reporting fields used when a search or discovery process supports manuscript content [Melissa L. Rethlefsen and the PRISMA-S Group, 2021].

The opening route visual turns the atlas handoff into a concrete reader choice: select the role, keep the evidence trace, and move to the next section with the right verifier question already named. See Figure 1.

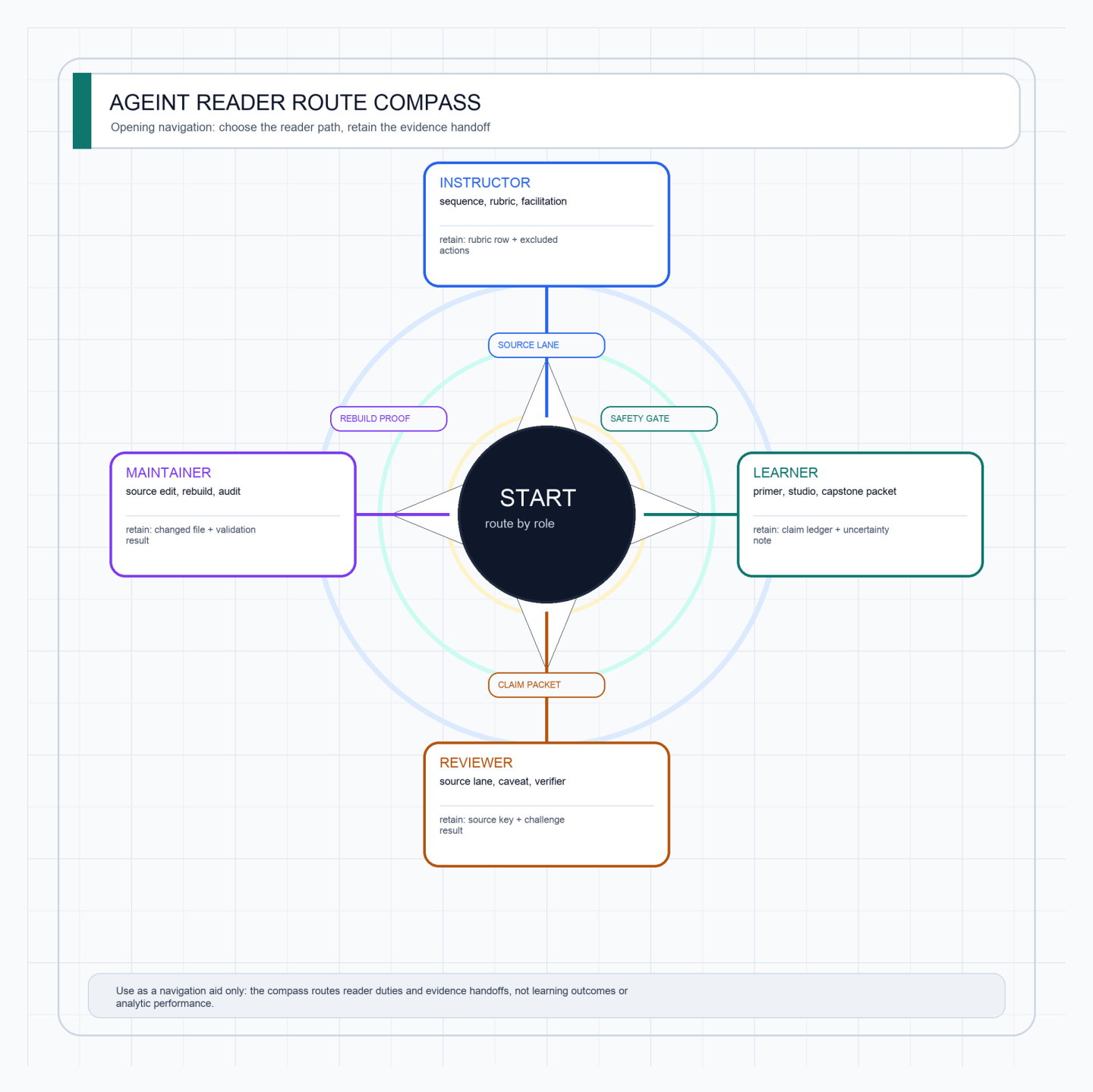


Figure 1: Opening navigation compass for the AGEINT orientation. It separates the instructor, learner, assurance reviewer, and maintainer routes and pairs each with the evidence trace that should survive the next reading move, so a reader can choose a path and know what to carry into the following section. It is navigation support, not a learning-outcome or performance claim.

2.2 Synthetic Analytic Tradecraft thesis: synthetic fixtures, source discipline, and reviewable claims

AGEINT is strongest when read as **Synthetic Analytic Tradecraft**: a governed practice for using synthetic inputs, generated artifacts, and bounded agentic assistance to make analytic reasoning inspectable before any real-world action is considered. The synthetic layer supplies safe fixtures: toy records, public declassified examples, instructor-provided evidence cards, owned-lab logs, and rendered figures. The tradecraft layer supplies the harder standard: source description, alternative hypotheses, assumption checks, probability/confidence separation, dissent, and reviewer challenge [of the Director of National Intelligence, 2015]; [Agency, 2009]; [Jr., 2007].

This framing tells you exactly what to expect — and what not to. AGEINT is not an operational manual and not a benchmark proving autonomous analytic performance. It is a source-governed workbench for producing reviewable analytic artifacts under synthetic conditions. The relevant question is whether a module can leave behind a traceable evidence packet that another analyst, instructor, or assurance reviewer can challenge: source keys, caveats, assumptions, alternatives, confidence basis, negative controls, rights constraints, and refresh triggers.

One short example makes the standard concrete. Studying a synthetic leaked-document fixture, a learner does not write *the document is authentic*. They write a packet: *source* = the synthetic tabletop fixture they were given; *claim type* = provenance assessment; *confidence* = moderate, because the metadata is internally consistent but cannot be independently checked; *alternative* = the document was fabricated to mislead; *refresh trigger* = re-open the judgment if a primary source is released. That record — not the verdict — is the deliverable AGEINT teaches.

The tradecraft figures make this claim visible, and all are assembled together in Section 2.34: the governed system map Figure 18 shows the whole governed stack; the analytic evidence ladder Figure 121 separates doctrine, reform, postmortem, empirical, and forecasting evidence; the SAT evidence boundary Figure 122 prevents universal debiasing claims; the SAT method contract Figure 19 binds source-family triangulation (the same point supported by more than one independent *kind* of source — an official standard *and* a peer-reviewed study, say, not two blog posts), synthetic fixtures, analytic field separation, negative-control testing, reviewer challenge, and artifact-evidence reporting; and the first-principles decomposition Figure 123 forces observation, inference, assumption, likelihood, confidence, dissent, and decision boundary fields to remain separate.

These four commitments are the reader-facing grouping of the six contract fields drawn in Figure 19: source-family triangulation and synthetic fixtures sit under the first two rows below, analytic-field separation and negative-control testing under the next two, and reviewer challenge and artifact-evidence reporting under the last two.

SAT commitment	How AGEINT implements it	Early audit surface
Synthetic before operational	Exercises use classroom fixtures, public or declassified examples, owned-lab traces, and tabletop records.	Section 2.36 and Section 2.13
Tradecraft before automation	Agent assistance must preserve source descriptors, alternatives, assumptions, probability/confidence boundaries, and reviewer challenge.	Figure 122 and Section 3
Evidence packet before claim	Claims need source keys, caveats, source-family triangulation, claim-calibration review, and refresh duties before reuse.	Figure 19, Figure 17, and Figure 23
Negative control before trust	Validators, rubrics, rendered PDFs, and figure registries are treated as attackable artifacts.	Figure 128 and Section 2.33

The workbench visual makes the Synthetic Analytic Tradecraft thesis inspectable by showing how safe fixtures become reviewable claim packets rather than operational instructions; it is a classroom artifact route, not evidence of field capability. See Figure 2.

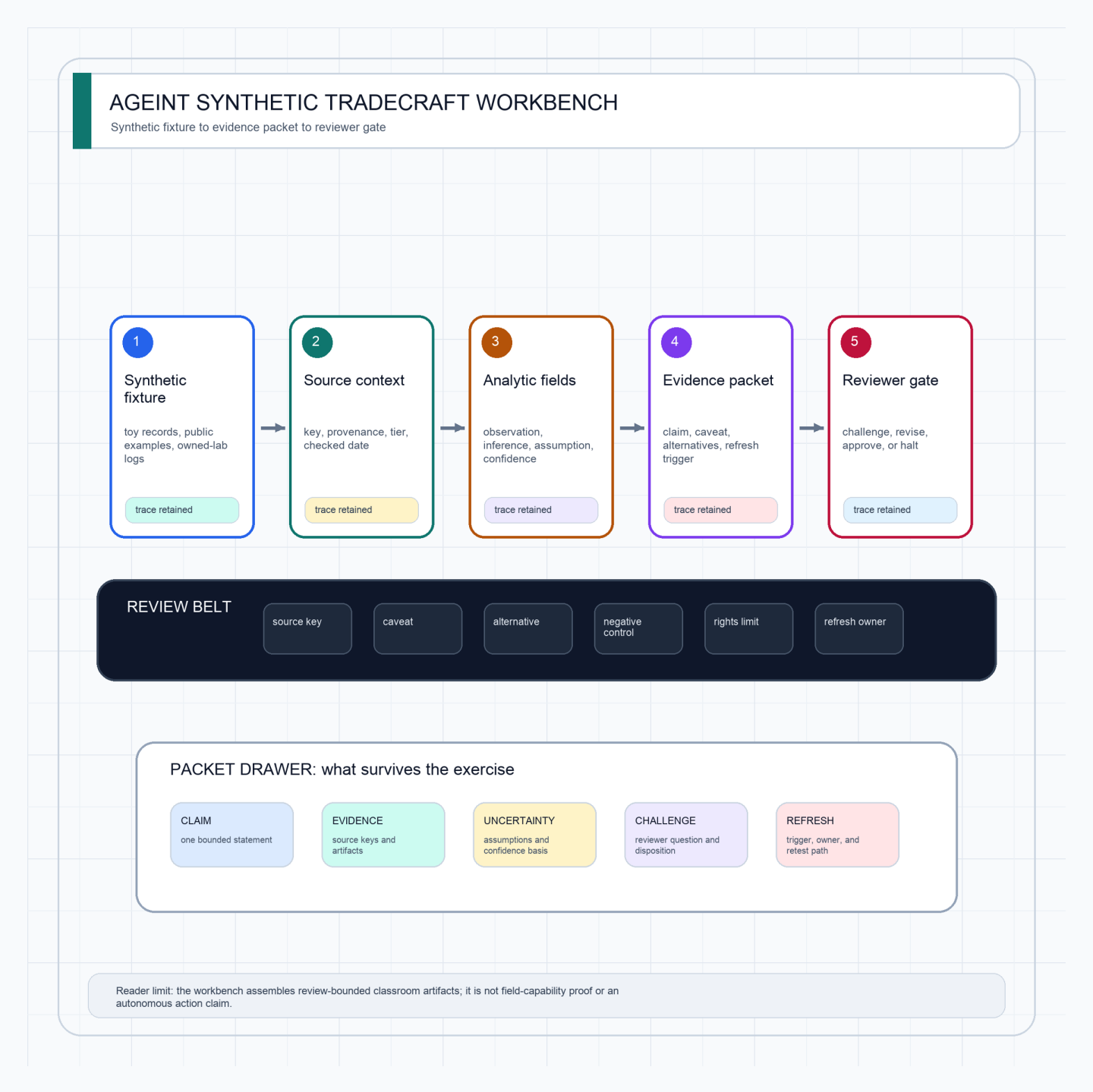


Figure 2: Workbench-style assembly line for Synthetic Analytic Tradecraft. It shows how a synthetic fixture becomes a source description, an analytic field set, a bounded claim packet, and a reviewer-gate disposition, tracing the path a classroom exercise takes from raw material to a record another analyst can challenge. It is a classroom artifact route, not an autonomous action claim or field-capability proof.

2.3 Reader paths: instructor, learner, reviewer, and maintainer handoffs

Reader	Fast path	Evidence to keep
Instructor	Pair the linked part introduction from Section 2.4 with each module's overview, practice studio, evidence contract, and governance boundary, confirm role ownership in Section 2.22, then set the assessment route from Section 2.20 before assigning a studio exercise built toward Section 2.14.	rubric row, excluded-action note, and source refresh trigger
Learner	Follow the module sequence from primer to practice studio, evidence contract, and governance boundary, then meet the assessment route in Section 2.20 before drafting a capstone packet against Section 2.14.	claim ledger entry, uncertainty note, and blocked-use statement
Assurance reviewer	Trace each material claim through Section 2.12, Section 80, Section 2.18, Section 2.34, and Section 2.33.	source key, review owner, caveat, and reproducible artifact path
Builder or maintainer	Treat generated output as an audit surface; update data, templates, manifest code, or figure specs, then rebuild and compare verifier reports.	changed source file, regeneration command, and validation result

2.4 Curriculum map: parts, modules, and source-backed route choices

Curriculum area	Part intro	Modules	Unit map	Runtime source
Foundations of Intelligence Tradecraft	Section 4	3	Figure 30	parsed source guide
Human Intelligence (HUMINT)	Section 8	3	Figure 36	parsed source guide
Signals Intelligence (SIGINT)	Section 12	2	Figure 41	parsed source guide
Open Source Intelligence (OSINT)	Section 15	3	Figure 45	parsed source guide
Technical Intelligence and Cyber Operations	Section 19	4	Figure 52	parsed source guide
Imagery and Financial Intelligence	Section 24	2	Figure 58	parsed source guide
Psychological Operations and Influence	Section 27	4	Figure 64	parsed source guide
Counterintelligence	Section 32	2	Figure 70	parsed source guide
Gray Zone, Hybrid Warfare, and Non-state Actors	Section 35	3	Figure 74	parsed source guide
Historical Intelligence Services	Section 39	4	Figure 79	parsed source guide
AGEINT — Agentic Intelligence	Section 44	6	Figure 85	parsed source guide
Cognitive Security	Section 51	4	Figure 107	parsed source guide
Epistemic Rigor and Analytic Tradecraft	Section 56	2	Figure 116	parsed source guide
Productivity Intelligence and Cognitive Performance	Section 59	2	Figure 129	parsed source guide
Industrial and Cyber-physical Intelligence	Section 62	5	Figure 134	parsed source guide
Legal, Ethical, and Oversight Frameworks	Section 68	2	Figure 143	parsed source guide

2.5 Runtime inventory: generated counts, anchors, and method appendices

These counts describe the size of the build, not its quality. They let a maintainer confirm a rebuild produced the expected inventory and let a reader gauge scope; they are not a performance, coverage, or learning-outcome claim (see Section 2.32).

Derived artifact	Runtime value
Curriculum parts	16
Curriculum modules	51
Methods appendices	9
AGEINT patterns	20
Parsed references	312
Official source-quality anchors	10
Intelligence research anchors	462
Intelligence practice lenses	14

The source constellation visual ties the runtime inventory back to the evidence families and lanes that govern source choice, caveat language, and refresh duties. See Figure 3.

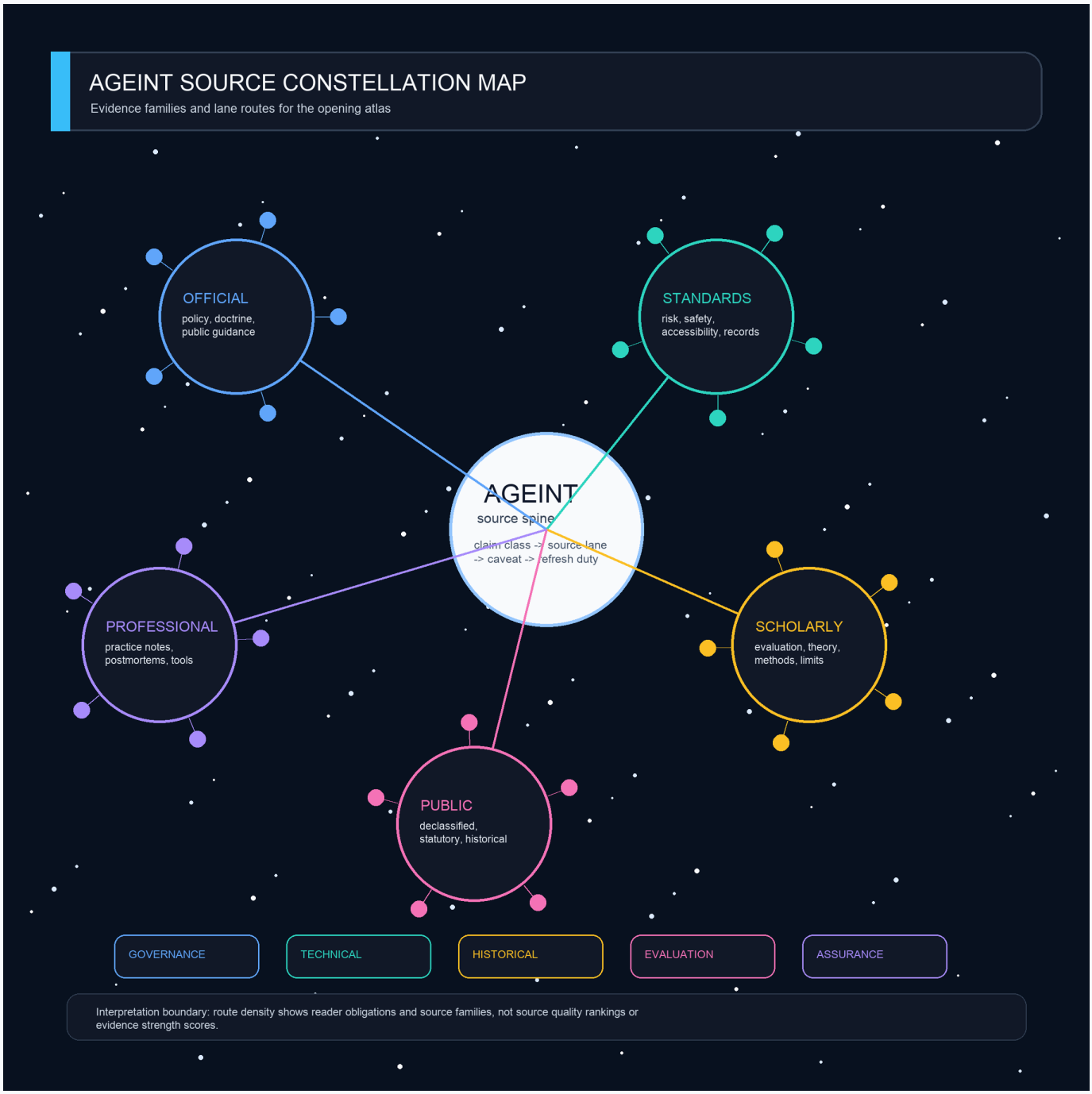


Figure 3: Source-family constellation for early orientation. It places the official, standards, scholarly, public, and professional evidence families around the AGEINT source spine so a reader can route governance, technical, historical, evaluation, and assurance claims to the lane whose evidence actually supports them. Route density shows coverage, not a ranking of source quality or evidence strength.

2.6 Related work and contribution boundary: adjacent literatures and AGEINT limits

AGEINT sits between several bodies of work rather than inside only one of them: AI risk-management guidance, generative-AI profiles, public-sector agentic-AI controls, model and dataset documentation practices, active-inference theory, agent security, and source-reporting methods [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]; [of Canada Secretariat, 2026a]; [Margaret Mitchell and Gebru, 2019]; [Timnit Gebru and Crawford, 2021]; [Mahima Pushkarna and Kjartansson, 2022]; [Friston, 2010]; [Christopher L. Buckley and Seth, 2017]; [Kai Greshake and Fritz, 2023]; [Melissa L. Rethlefsen and the PRISMA-S Group, 2021]. Its contribution is not a new agent architecture, cognitive theory, attack benchmark, or measured learning outcome. The contribution is a versioned curriculum-and-assurance framework that links source identity, claim classes, safe exercises, figures, capstone artifacts, and rebuildable review gates for bounded agentic-intelligence education.

The four-domain convergence map Figure 8 makes that boundary visible. Synthetic-intelligence support is treated as useful only when analytic tradecraft standards, OPSEC and zero-trust constraints, and cognitive-security safeguards remain separate review gates [Dylan and Stivang, 2025]; [Caballero and Jenkins, 2024]; [McMahon, 2024]; [The White House, 1988]; [of Standards and Technology, 2020b]; [Wardle and Derakhshan, 2017]; [Terp and Breuer, 2022]. The map therefore routes AI, OPSEC, and cognitive-security claims into source-backed classroom artifacts while blocking autonomous strategic-judgment claims, manipulation guidance, live-targeting workflows, and unsupported efficacy claims.

2.7 Analysis validation protocol: claim classes, evidence packets, and failure modes

The manuscript now treats analysis validation as a reader-facing method, not a private build habit. Each major claim class must name the evidence packet that would make it reviewable, the validation question a reviewer should ask, and the failure mode that would force warning or remediation. The analysis validation matrix Figure 20 is the compact visual form of that protocol: design guidance needs a source family and caveat; empirical or evaluation claims need a study, metric, or benchmark; governance claims need law, standard, or rights-impact support; figure claims need registry text, rendered pixels, and link-safe PDF output; artifact-readiness claims need fresh builds and current audits; reviewer dispositions need a task ledger and negative control.

The claim-calibration verifier adds the machine-checkable edge to that protocol Figure 23. Artifact telemetry such as citation counts, figure counts, page counts, link counts, and validator pass states is useful readiness evidence, but it is not a statistical result, learning-outcome estimate, operational-performance benchmark, or universal safety claim. The audit therefore fails unsupported proof-language, measured-performance claims, p-value or significance language, and decorative formalisms without direct support and limitation text, while allowing explicit boundary language and misconception checks that warn the reader what a source cannot establish.

Claim class	Validation question	Required evidence	Failure mode
Design guidance	Is the claim framed as proposed guidance rather than measured performance?	source-family support, caveat, and bounded conclusion	architecture prose is promoted into empirical proof
Empirical or evaluation claim	Does a cited study, metric, benchmark, or evaluation source directly support the claim?	method source, limitation note, and refresh trigger	measured language appears without direct evaluation evidence
Governance or rights claim	Which law, standard, public guidance, or rights-impact source constrains the advice?	source lane, affected group, owner, residual risk	compliance language appears as unsupported assurance
Figure or visualization claim	Does the visual carry readable text, alt text, provenance, and an inspectable source section?	registry row, PNG metadata, caption, long description	a figure works only as decoration or inaccessible evidence
Artifact readiness claim	Are manuscript, citations, figures, references, and PDF links from the same rebuild?	artifact-evidence manifest, rendered-reference audit, PDF audit	stale output or Markdown-file links certify as ready
Reviewer disposition	What would make this row pass, warn, fail, or reopen?	negative control, closure evidence, task owner	a green check hides the decision rule

The assurance cockpit visual summarizes how a reader should interpret local build telemetry: useful for routing review effort, but bounded by the generated audits that carry the authoritative pass, warn, or block state. See Figure 4.

Figure 4: Audit-tile orientation cockpit for local readiness. It groups build freshness, reference quality, source metadata, refresh posture, figure quality, and the publication-readiness boundary into reader-facing tiles that route review effort to the right verifier. The tiles are schematic orientation only; authoritative status — the pass, warn, or block state — lives in the generated audits, not in this figure.

2.8 Consolidated glossary and index: terms, audit surfaces, and reader routing

Use this compact index to route common terms to the right audit surface before reading a chapter in detail.

Term	Working meaning	Primary audit surface
Source lane	The provenance, source tier, and refresh context that govern a claim.	Section 2.12 and Section 80
Source tier	The evidence role assigned to a source: official, standards, scholarly, practitioner, vendor, historical, or source-guide context.	Section 2.11 and source annotations
Synthetic Analytic Tradecraft	The controlled use of synthetic fixtures and bounded agent support to make analytic reasoning, evidence, uncertainty, dissent, and review gates inspectable.	Section 2.2 and Figure 19
Analysis validation	The review protocol that maps claim class, validation question, evidence packet, failure mode, and disposition before a claim can be treated as ready.	Section 2.7 and Figure 20
Claim ledger	A reviewable record of claim, evidence, caveat, confidence, and owner.	Section 2.32 and Section 2.14
Safe substitution	A replacement of unsafe operational action with synthetic, public, tabletop, or governance work.	Section 2.13
Reviewer gate	A named human approval or challenge point before reuse, presentation, or tool execution.	Section 2.20 and Section 2.23
Figure registry	The reproducible map from figure label to generated asset, caption, and source section.	Section 2.34

2.9 Intelligence research profiles: domain lanes, source roles, and profile routing

Profile	Anchor count	Core contract
Governed Intelligence Cycle and Dissemination Architecture	58	requirements, data provenance, analytic judgments, markings, dissemination permissions, records obligations, and feedback remain separable artifacts
Analytic Tradecraft and Source Integrity	110	every agent output must preserve evidence, assumptions, judgments, likelihood, confidence, dissent, empirical limits, and change history as separable fields
AI Ethics, Data Governance, and Civil-Liberties Review	78	data, model, prompt, output, evaluator, accountable human, audit evidence, and retention rule are independently inspectable and versioned
Agentic AI Governance and Tool Security	106	agents, tools, credentials, memory, retrieval stores, policies, and logs remain separately inspectable and revocable components
Open-Source and Geospatial Intelligence Integrity	51	collection notes, source metadata, transformations, caveats, and analytic judgments remain separately exportable
Collection Management and Multi-INT Requirements Discipline	58	requirements, authorities, source disciplines, collection notes, retention limits, caveats, and evaluation metrics remain separable
Financial Intelligence and Economic-Security Due Diligence	37	entities, transactions, sanctions programs, red flags, supplier evidence, legal constraints, and analytic judgments remain separately reviewable
Counterintelligence and Source-Integrity Defense	55	identity, access, reporting, corroboration, caveats, and confidence are modeled independently so defensive review can happen without exposure
Cognitive Security and Influence Resilience	62	separate descriptive analysis, normative assessment, response options, and protected-audience considerations
Active-Inference Theory and Governed Agent Analogy	12	formal claim, pedagogical analogy, implementation assumption, evaluation evidence, and governance duty remain distinct fields
Historical and Declassified Intelligence Services	22	archive source, release channel, historical context, analytic lesson, oversight implication, and modern analogy remain explicitly separated
Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense	69	indicators, TTP mappings, affected assets, supplier evidence, response actions, and sharing constraints remain independently reusable
ICS/OT Cyber-Physical Defense and Tabletop Readiness	33	separate cyber indicators, engineering observations, safety impacts, operator decisions, and recovery actions
Legal, Ethical, and Oversight Architecture	74	policies, approvals, audit logs, evidence, and action permissions remain linked but independently inspectable
Operator Productivity and Cognitive Performance	3	requirements queues, workload signals, focus blocks, evidence packets, and reviewer checkpoints remain separable artifacts

2.10 Intelligence practice lenses: artifact expectations, safety checks, and review questions

Practice lens	Evidence artifact	Validation rule	Safety check
Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	verify source authority, public/classification status, CAPCO-safe vocabulary, audience need, and records disposition before reuse	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	show priority, authority, minimization, corroboration, and source quality before any claim is reused	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
AI/Data Accountability Lens	AI/data impact card with authority, provenance, model version, impact score, register status, human owner, and review cadence	confirm lawful data use, limitations, bias and accuracy testing, public-register fit, human accountability, and rights escalation	reject automated adverse action, hidden surveillance expansion, unowned outputs, unreviewed model drift, and opaque downstream reuse
Active-Inference Boundary Lens	theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition	separate formal claim, pedagogical analogy, implementation assumption, evaluation evidence, and governance duty before reuse	reject claims that the free-energy principle proves autonomous agency, intent, detection performance, or oversight-free action
Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	separate raw reporting, inference, judgment, and recommendation before synthesis	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Operator-Workload Hygiene Lens	operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary	separate urgency from authority, workload from quality, and personal tempo claims from measured task-switching cost	exclude live operational tempo mandates, surveillance of people, performance coercion, and unreviewed tasking under fatigue
Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	distinguish what the record shows, what remains redacted or unknown, and which governance lesson is defensibly transferable	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Economic-Security Due-Diligence Lens	economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary	verify official list source, typology provenance, beneficial-ownership uncertainty, export-control relevance, and non-evasion framing	exclude sanctions evasion, laundering methods, threshold gaming, procurement bypasses, and tailored targeting of real firms
Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	verify least privilege, prompt-injection exposure, provenance, observability, stop conditions, and incident-reporting triggers	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Defensive Cyber-Intelligence Lens	defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication	verify that taxonomy labels are descriptive, indicators are contextualized, incident categories are reviewable, and outputs remain detection or assurance oriented	exclude exploit steps, evasion instructions, malware construction, credential misuse, phishing instructions, and live response actions
Software-Supply-Chain Assurance Lens	software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps	separate provenance evidence, social-trust signals, build controls, vulnerability claims, and attribution uncertainty	exclude exploit reproduction, maintainer targeting, backdoor mechanics, credential hunting, and live repository interference
Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	distinguish observation, attribution, impact assessment, and resilience response	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	validate against safety, availability, engineering state, incident scope, and after-action learning	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	confirm lawful purpose, proportionality, retention, review, and appeal or redress paths	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought

2.11 Research anchor atlas: curated sources, lanes, tiers, and claim scope

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Agency, 2009]	analytic_tradecraft	analytic_tradecraft	official_primary	2026-05-21	annual	Official structured analytic techniques primer for bias checks, alternatives, and warning analysis.
[Agency, 2016]	analytic_tradecraft	analytic_tradecraft	official_primary	2026-05-21	annual	Defense intelligence structured-analysis primer for classroom analytic exercises.
[of the Director of National Intelligence, 2026d]	analytic_tradecraft	analytic_tradecraft	official_primary	2026-05-21	annual	Official sourcing directive for traceability, citations, source descriptors, and source summaries.
[of the Director of National Intelligence, 2026e]	analytic_tradecraft	analytic_tradecraft	official_primary	2026-05-21	annual	Official ODNI explanation of analytic objectivity, ombuds, and tradecraft standards.
[of State, 2024]	osint_geoint	osint_geoint	official_primary	2026-05-21	annual	Official strategy source for lawful OSINT governance, discovery, validation, and dissemination.
[Jr., 2007]	analytic_tradecraft	analytic_tradecraft	scholarly_or_official	2026-06-06	annual	Foundational analytic cognition source for bias, mental models, and structured reasoning.
[of the Director of National Intelligence, 2026c]	collection_management	collection_management	official_primary	2026-05-21	annual	Official prioritization directive for translating national intelligence priorities into collection, analysis, risk management, and responsiveness evaluation.
[of Staff, 2026]	collection_management	collection_management	official_primary	2026-05-21	annual	Official joint-doctrine landing page for the keystone publication on joint intelligence principles, products, services, and assessments.
[of the Army, 2020]	analytic_tradecraft	analytic_tradecraft	official_primary	2026-05-21	annual	Official Army analytic doctrine for intelligence-analysis process, structured analytic techniques, analytic design, and cognitive discipline.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Counterintelligence and Center, 2024]	counterintelligence_source_integrity	counterintelligence_source_integrity	official_primary	2026-05-21	annual	Official strategy for defensive CI integration, foreign-intelligence threat awareness, strategic advantage protection, and future readiness.
[of the Director of National Intelligence and Agency, 2024]	osint_geoint	osint_geoint	official_primary	2026-05-21	annual	Official IC OSINT strategy for professionalizing OSINT, integrated collection management, open-source sharing, innovation, and tradecraft.
[Agency, 2026c]	osint_geoint	osint_geoint	official_primary	2026-05-21	annual	Official NGA strategy anchor for GEOINT readiness, warning, partnership resilience, resource stewardship, and AI integration.
[Archives and Administration, 1981]	legal_oversight	legal_oversight	official_primary	2026-05-21	annual	Official legal anchor for intelligence authorities, rights-aware collection, analytic competition, oversight, and source-method protection.
[Agency, 2026g]	legal_oversight	legal_oversight	official_primary	2026-05-21	annual	Official NSA public explanation of FISA oversight for signals intelligence collection governed by statutory and court-authorized controls.
[Community, 2026]	governed_intelligence_cycle	governed_intelligence_cycle	official_primary	2026-05-21	annual	Official public explanation of the intelligence cycle, collection disciplines, dissemination, evaluation, oversight, and partners.
[Community, 2020b]	ai_ethics_data_governance	ai_ethics_data_governance	official_primary	2026-05-21	annual	Official IC principles for lawful, accountable, objective, human-centered, secure, resilient, and science-informed AI.
[Community, 2020a]	ai_ethics_data_governance	ai_ethics_data_governance	official_primary	2026-05-21	annual	Official IC framework for AI goals, authorities, human judgment, bias mitigation, testing, documentation, explainability, and review.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[of the Director of National Intelligence, 2025b]	ai_ethics_data_governance	ai_ethics_data_governance	official_primary	2026-05-21	annual	Official IC AI governance directive covering CAIO roles, oversight, interoperability, civil-liberties review, training data, and impact assessment.
[of the Director of National Intelligence, 2025a]	ai_ethics_data_governance	ai_ethics_data_governance	official_primary	2026-05-21	annual	Official IC data-management directive for data governance, data stewardship, CDO authority, interoperability, and data lifecycle management.
[of the Director of National Intelligence, 2026b]	governed_intelligence	governed_intelligence	official_primary	2026-05-21	annual	Official CAPCO register for classification and control-marking vocabulary, abbreviations, portion markings, and dissemination syntax.
[Privacy and Board, 2026]	legal_oversight	legal_oversight	official_primary	2026-05-21	annual	Official oversight-report library for privacy, civil-liberties, surveillance, watchlisting, facial-recognition, and redress analysis.
[General Services Administration et al., 2026]	ai_ethics_data_governance	ai_ethics_data_governance	official_primary	2026-05-21	annual	Official federal data-governance benchmark for data as a strategic asset, ethical governance, lifecycle practices, and learning culture.
[Agency, 2026a]	historical_declassified_sources	historical_declassified_sources	official_primary	2026-05-21	annual	Official CSI landing page for Studies in Intelligence, declassified professional reflection, analytic history, and institutional learning.
[Agency, 2026h]	historical_declassified_sources	historical_declassified_sources	official_primary	2026-05-21	annual	Official declassified historical-release library for cryptologic history, SIGINT history, COMSEC, oral histories, and historical cases.
[Office, 2026a]	historical_declassified_sources	historical_declassified_sources	official_primary	2026-05-21	annual	Official declassified satellite-reconnaissance program archive for CORONA, GAMBIT, POPPY, QUILL, and other historical technical-intelligence cases.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Archives and Administration, 2026b]	historical_declassified_sources	historical_declassified_sources	official_primary	2026-05-21	annual	Official NARA guide to CIA Record Group 263, archival provenance, record series, and declassified intelligence research pathways.
[Network, 2026a]	financial_economic_security	financial_economic_security	official_primary	2026-05-21	annual	Official FININT source for AML/CFT advisories, typology awareness, sanctions-evasion warnings, red flags, and compliance-oriented monitoring.
[of Foreign Assets Control, 2026]	financial_economic_security	financial_economic_security	official_primary	2026-05-21	annual	Official OFAC sanctions-program library for understanding legal program structure, list maintenance, and compliance-oriented economic statecraft.
[Force, 2025]	financial_economic_security	financial_economic_security	international_standard	2026-05-21	annual	Official international AML/CFT/CPF standard for risk-based controls, beneficial ownership, information sharing, supervision, and mutual evaluation.
[of Industry and Security, 2026]	financial_economic_security	financial_economic_security	official_primary	2026-05-21	annual	Official export-control enforcement source for compliance, screening, red flags, voluntary disclosures, and national-security protection of sensitive items.
[Authority, 2026]	agentic_ai_governance	agentic_ai_governance	official_primary	2026-05-21	annual	Government framework focused on agentic AI delegation, controls, and safe deployment.
[ASD ACSC and NCSC-UK, 2026]	agentic_ai_governance	agentic_ai_governance	official_primary	2026-05-21	annual	Joint government guidance for deploying agentic AI with identity, logging, and progressive controls.
[of Standards and Technology, 2026a]	agentic_ai_governance	agentic_ai_governance	official_primary	2026-05-21	annual	NIST concept paper for applying identity and authorization standards to software and AI agents.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[of Standards and Technology, 2026c]	agentic_ai_governance	agent_interoperability_standards	official_primary	2026-06-11	quarterly	Official NIST initiative for trusted, interoperable, and secure AI-agent standards, protocols, identity, and evaluation research.
[UK Department for Science et al., 2024]	agentic_ai_governance	agentic_ai_governance	official_primary	2026-05-21	annual	Official evaluation guidance for advanced AI systems, including agent evaluations for tool use, semi-autonomy, and real-world actions.
[Project, 2026b]	agentic_ai_governance	agentic_ai_security	security_standard	2026-06-11	semiannual	OWASP GenAI Security Project resource identifying critical risks and mitigations for autonomous and agentic AI applications.
[MITRE, 2026a]	agentic_ai_governance	ai_red_team_assurance	research_standard	2026-06-11	quarterly	MITRE ATLAS is a living knowledge base for adversarial threats to AI-enabled systems, useful for defensive red-team mapping and control coverage.
[Project, 2025d]	agentic_ai_governance	agentic_ai_governance	security_standard	2026-05-21	annual	Security taxonomy for prompt injection, excessive agency, data leakage, and LLM application risks.
[of Standards and Technology, 2022d]	agentic_ai_governance	agentic_ai_governance	official_primary	2026-05-21	annual	Official secure development framework for agent tooling, connectors, and software supply chains.
[of Standards and Technology, 2024f]	ics_ot_defense	ics_ot_defense	official_primary	2026-05-21	annual	Official cybersecurity-risk governance framework that adds the Govern function and supplies a common language for AI, OT, and enterprise risk.
[of Standards and Technology, 2022b]	ics_ot_defense	ics_ot_defense	official_primary	2026-05-21	annual	Systems-security engineering foundation for trustworthy systems in contested operational environments and related training programs.
[of Standards and Technology, 2016]	cyber_threat_intelligence	cyber_threat_intelligence	official_primary	2026-05-21	annual	Official guidance for establishing threat-information sharing goals, communities, distribution rules, and defensive use of indicators and TTPs.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[of Standards and Technology, 2025c]	cyber_threat_intelligence	cyber_threat_intelligence	official_primary	2026-05-21	annual	Official incident-response profile for preparation, detection, response, recovery, and continuous improvement under CSF 2.0.
[of Standards and Technology, 2022c]	cyber_threat_intelligence	cyber_threat_intelligence	official_primary	2026-05-21	annual	Official supply-chain risk-management guidance for identifying, assessing, and mitigating product, service, vendor, and process risks.
[Cybersecurity and Agency, 2026c]	ics_ot_defense	ics_ot_defense	official_primary	2026-05-21	annual	Official defensive ICS practice library for defense-in-depth, forensics, incident response, and remote access.
[Cybersecurity and Agency, 2026f]	ics_ot_defense	ics_ot_defense	official_primary	2026-05-21	annual	Official exercise packages for cyber, physical, ICS, ransomware, and convergence tabletop scenarios.
[of Standards and Technology, 2006]	ics_ot_defense	ics_ot_defense	official_primary	2026-05-21	annual	Official methodology for designing, conducting, and evaluating test, training, and exercise programs.
[MITRE, 2026c]	ics_ot_defense	ics_ot_defense	research_standard	2026-05-21	annual	Threat-informed defensive matrix for ICS tactics and techniques, used for coverage mapping.
[for Security Policy, 2025]	cognitive_influence_security	cognitive_influence_security	scholarly_policy	2026-05-21	annual	Policy-scholarship source for cognitive security, information literacy, critical thinking, and whole-of-society resilience.
[NSA and partners, 2025]	ics_ot_defense	ics_ot_defense	official_primary	2026-05-21	annual	Joint government guidance for AI governance, assurance, safety, and security in OT environments.
[Foundation, 2026]	agentic_ai_governance	agentic_ai_governance	official_primary	2026-05-21	annual	Official NSF source for open AI-agent protocol ecosystems, interoperability, identity, access control, auditability, and safe message formats.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[for Disease Control and Prevention, 2026]	agentic_ai_governance	agentic_ai_governance	official_primary	2026-05-21	annual	Official public-health guidance for scoping agentic research, human oversight, expert validation, sensitive-data avoidance, and non-replacement of professional judgment.
[of Standards and Technology, 2026f]	ai_ethics_data_governance	ai_ethics_data_governance	official_primary	2026-05-21	annual	Official AI RMF playbook for translating Govern, Map, Measure, and Manage functions into curriculum controls and review prompts.
[OECD, 2024]	ai_ethics_data_governance	ai_ethics_data_governance	international_standard	2026-05-21	annual	Official OECD principles for human-centered values, robustness, transparency, accountability, and inclusive AI growth.
[for Standardization, 2023b]	ai_ethics_data_governance	ai_ethics_data_governance	international_standard	2026-05-21	annual	International AI management-system standard for responsible AI governance, traceability, transparency, risk, and continual improvement.
[for Standardization, 2023a]	ai_ethics_data_governance	ai_ethics_data_governance	international_standard	2026-05-21	annual	International guidance for integrating AI-specific risk management into organizational activities, products, systems, and services.
[of Europe, 2024]	legal_oversight	legal_oversight	official_primary	2026-05-21	annual	Official treaty anchor for human rights, democracy, rule-of-law, risk management, accountability, and public-sector AI governance.
[Office, 2025]	privacy_ip_governance	privacy_ip_governance	official_primary	2026-05-21	annual	Official U.S. copyright policy source for generative-AI training, rights-holder impacts, transparency, licensing, and IP governance.
[of Standards and Technology, 2020b]	agentic_ai_governance	agentic_ai_governance	official_primary	2026-05-21	annual	Official zero-trust architecture guidance for identity-centric authorization, continuous evaluation, least privilege, and policy enforcement.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[of Standards and Technology, 2025b]	agentic_ai_governance	agentic_ai_governance	official_primary	2026-05-21	annual	Official digital-identity guidance for authentication, federation, identity proofing, and agent/tool authorization analogies.
[IETF, 2025]	agentic_ai_governance	agentic_ai_governance	internet_standard	2026-05-21	annual	Internet standards-track security guidance for OAuth deployment, token protection, redirect safety, and authorization hardening.
[IETF, 2023]	agentic_ai_governance	agentic_ai_governance	internet_standard	2026-05-21	annual	Internet standard for sender-constrained OAuth tokens, useful for agent tool-call identity and credential-binding discussions.
[of Standards and Technology, 2012]	legal_oversight	legal_oversight	official_primary	2026-05-21	annual	Official risk-assessment method for threat, vulnerability, impact, likelihood, uncertainty, and residual-risk reasoning.
[of Standards and Technology, 2018b]	legal_oversight	legal_oversight	official_primary	2026-05-21	annual	Official RMF lifecycle source for preparation, categorization, control selection, implementation, assessment, authorization, and monitoring.
[of Standards and Technology, 2011a]	cyber_threat_intelligence	cyber_threat_intelligence	official_primary	2026-05-21	annual	Official continuous-monitoring guidance for metrics, status awareness, ongoing authorization, and governance feedback loops.
[of Standards and Technology, 2011b]	legal_oversight	legal_oversight	official_primary	2026-05-21	annual	Official enterprise-risk source for mission, organization, and system tiers, risk framing, assessment, response, and monitoring.
[of Standards and Technology, 2021]	counterintelligence_source_integrity	counterintelligence_source_integrity	official_primary	2026-05-21	annual	Official enhanced security requirements for high-value CUI, source handling analogies, system integrity, and advanced persistent threat resistance.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[of Standards and Technology, 2022a]	ai_ethics_data_governance	ai_ethics_data_governance	official_primary	2026-05-21	annual	Official NIST source for AI bias concepts, socio-technical framing, measurement limits, and governance-oriented mitigation.
[Committee, 2025]	cyber_threat_intelligence	cyber_threat_intelligence	international_standard	2026-05-21	annual	OASIS CTI standard for expressing cyber threat and observable information with structured objects, relationships, sightings, and markings.
[Committee, 2021]	cyber_threat_intelligence	cyber_threat_intelligence	international_standard	2026-05-21	annual	OASIS CTI transport standard for defensive threat-intelligence exchange channels, collections, discovery, and API contracts.
[MITRE, 2026b]	cyber_threat_intelligence	cyber_threat_intelligence	research_standard	2026-05-21	annual	Threat-informed enterprise matrix for defensive TTP mapping, coverage analysis, detection engineering, and analytic normalization.
[Cybersecurity and Agency, 2026a]	ics_ot_defense	ics_ot_defense	official_primary	2026-05-21	annual	Official prioritized baseline of IT and OT cybersecurity practices for critical-infrastructure risk reduction and maturity assessment.
[Cybersecurity and Agency, 2026e]	agentic_ai_governance	agentic_ai_governance	official_primary	2026-05-21	annual	Official secure-by-design program source for customer security outcomes, radical transparency, leadership accountability, and safer defaults.
[Cybersecurity and Agency, 2026d]	cyber_threat_intelligence	cyber_threat_intelligence	official_primary	2026-05-21	annual	Official catalog for prioritizing known exploited vulnerabilities as defensive triage inputs, not as exploitation instructions.
[Agency, 2026b]	osint_geoint	osint_geoint	official_primary	2026-05-21	annual	Official NGA source on GEOINT AI, data quality, model performance, interoperability, analyst interaction, and standards leadership.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[for Standardization, 2013]	osint_geoint	osint_geoint	international_standard	2026-05-21	annual	International geospatial data-quality standard for completeness, logical consistency, positional accuracy, temporal quality, and usability framing.
[Cybersecurity and Agency, 2026b]	cognitive_influence_security	cognitive_influence_security	official_primary	2026-05-21	annual	Official CISA election-security source for public-resilience, foreign-influence awareness, rumor control, and defensive communication framing.
[Organization, 2026c]	cognitive_influence_security	cognitive_influence_security	official_primary	2026-05-21	annual	Official NATO source for hybrid-threat resilience across cyber, information, economic, political, and military pressure.
[OECD, 2026c]	cognitive_influence_security	cognitive_influence_security	official_primary	2026-05-21	annual	Official OECD policy source for information integrity, governance responses, public trust, and democratic resilience.
[Network, 2026b]	financial_economic_security	financial_economic_security	official_primary	2026-05-21	annual	Official FinCEN source for beneficial-ownership reporting, entity transparency, exemptions, and compliance-oriented analysis.
[of Foreign Assets Control, 2019]	financial_economic_security	financial_economic_security	official_primary	2026-05-21	annual	Official OFAC compliance framework for management commitment, risk assessment, internal controls, testing, auditing, and training.
[Force, 2021]	financial_economic_security	financial_economic_security	international_standard	2026-05-21	annual	Official FATF guidance for virtual-asset risk, VASP supervision, travel-rule compliance, and non-evasion FININT education.
[for International Settlements, 2021]	financial_economic_security	financial_economic_security	official_primary	2026-05-21	annual	Official BIS policy source for financial technology, market structure, data, network effects, regulation, privacy, and stability tradeoffs.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[of Standards and Technology, 2017]	ics_ot_defense	ics_ot_defense	official_primary	2026-05-21	annual	Official NIST cyber-physical systems framework for functions, timing, trustworthiness, interoperability, and safety-aware architecture.
[of Standards and Technology, 2018a]	ics_ot_defense	ics_ot_defense	official_primary	2026-05-21	annual	Official NCCoE practice guide for manufacturing-sector ICS integrity, monitoring, architecture, and defensive lab validation.
[Organization, 2026d]	privacy_ip_governance	privacy_ip_governance	official_primary	2026-05-21	annual	Official WIPO source for AI and IP policy, training-data rights, copyright infrastructure, transparency, attribution, and member-state dialogue.
[of Standards and Technology, 2026k]	privacy_ip_governance	privacy_ip_governance	official_primary	2026-05-21	annual	Official privacy risk-management framework for identifying and managing privacy risk, data governance, workforce roles, and enterprise controls.
[of Standards and Technology, 2020a]	legal_oversight	legal_oversight	official_primary	2026-05-21	annual	Official security and privacy control catalog for control baselines, assessment language, privacy controls, and inherited-control reasoning.
[of Standards and Technology, 2024]	legal_oversight	legal_oversight	official_primary	2026-05-21	annual	Official mapping-method source for comparing controls, regulations, frameworks, and guidance without collapsing their separate purposes.
[of Standards and Technology, 2024a]	agentic_ai_governance	agentic_ai_governance	official_primary	2026-05-21	annual	Official adversarial-ML taxonomy for defensive AI threat modeling, mitigation vocabulary, evaluation limits, and safe red-team framing.
[Commission, 2026b]	ai_conformity_compliance	ai_conformity_compliance	official_primary	2026-05-22	quarterly	Official European Commission source for AI Office responsibilities, GPAI oversight, enforcement coordination, codes of practice, and AI Act implementation.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Commission, 2026h]	ai_conformity_compliance	ai_conformity_compliance	official_primary	2026-05-22	quarterly	Official European Commission source for GPAI Code of Practice drafting, transparency, copyright, safety, security, and AI Act implementation support.
[Commission, 2026a]	ai_conformity_compliance	ai_conformity_compliance	official_primary	2026-05-22	quarterly	Official European Commission AI Act implementation page for risk tiers, prohibited practices, GPAI obligations, governance bodies, and phased application.
[for Standardization, 2025]	ai_conformity_compliance	ai_conformity_compliance	international_standard	2026-05-22	semiannual	ISO standard page for AI system impact assessment across lifecycle, stakeholder impact documentation, transparency, and accountability.
[for Standardization, 2020]	ai_conformity_compliance	ai_conformity_compliance	international_standard	2026-05-22	annual	ISO technical report page for AI trustworthiness terminology, approaches, engineering considerations, and governance vocabulary.
[Office, 2021]	ai_conformity_compliance	ai_conformity_compliance	official_primary	2026-05-22	annual	Official GAO accountability framework for AI governance, data, performance, monitoring, and accountability evidence.
[UNESCO, 2021]	human_rights_governance	human_rights_governance	international_standard	2026-05-22	annual	Official UNESCO recommendation source for human rights, fairness, transparency, accountability, education, culture, environment, and governance.
[of the United Nations High Commissioner for Human Rights, 2026a]	human_rights_governance	human_rights_governance	official_primary	2026-05-22	semiannual	Official OHCHR portal for human rights in digital space, including technology, privacy, civic space, equality, and remedy concerns.
[of the United Nations High Commissioner for Human Rights, 2026b]	human_rights_governance	human_rights_governance	official_primary	2026-05-22	semiannual	Official OHCHR privacy-in-the-digital-age page for surveillance, data protection, AI, remedy, and human-rights safeguards.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[of Europe, 2018]	human_rights_governance	human_rights_governance	official_primary	2026-05-22	annual	Official Council of Europe source for Convention 108+ privacy, data-protection principles, transborder flows, and supervisory cooperation.
[UNESCO, 2023]	education_assessment	education_assessment	official_primary	2026-05-22	annual	Official UNESCO publication for generative AI education governance, assessment integrity, age safeguards, teacher roles, and research use.
[UNESCO, 2024]	education_assessment	education_assessment	official_primary	2026-05-22	annual	Official UNESCO source for AI competency frameworks supporting teacher development, student capabilities, ethics, and curriculum design.
[Report, 2026]	education_assessment	education_assessment	official_primary	2026-05-22	semiannual	Official UNESCO GEM source hub for AI and education evidence, policy, access, assessment, and equity analysis.
[OECD, 2026b]	education_assessment	education_assessment	official_primary	2026-05-22	semiannual	Official OECD topic page for AI in education, learning systems, assessment, teacher support, and education policy.
[Commission, 2026g]	education_assessment	education_assessment	official_primary	2026-05-22	semiannual	Official European Commission source for digital education policy, digital skills, AI in education, teacher capacity, and assessment readiness.
[Observatory, 2026b]	public_sector_agentic_ai	public_sector_agentic_ai	official_primary	2026-06-06	semiannual	Official OECD.AI source for public-sector AI adoption, governance, public value, accountability, and government service transformation.
[GovTech and Team, 2026]	public_sector_agentic_ai	public_sector_agentic_ai	official_primary	2026-05-22	semiannual	Official World Bank GovTech source for public-sector AI policy instruments, implementation knowledge exchange, and inclusive government capacity.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Bank, 2026]	public_sector_agentic_ai	public_sector_agentic_ai	official_primary	2026-05-22	semiannual	Official World Bank GovTech program source for digital public infrastructure, citizen engagement, core systems, and public-sector modernization.
[Administration, 2026]	public_sector_agentic_ai	public_sector_agentic_ai	official_primary	2026-05-22	quarterly	Official U.S. government AI resource hub for agency adoption, responsible use, policy references, and public-sector implementation support.
[Commission, 2026e]	cross_border_data_spaces	cross_border_data_spaces	official_primary	2026-05-22	semiannual	Official European Commission source for data-sharing trust, data intermediaries, public-sector data reuse, data altruism, and European Data Spaces.
[Commission, 2026d]	cross_border_data_spaces	cross_border_data_spaces	official_primary	2026-05-22	semiannual	Official European Commission source explaining Data Act access, use, connected-product data, interoperability, and cross-sector data availability.
[Commission, 2026c]	cross_border_data_spaces	cross_border_data_spaces	official_primary	2026-05-22	semiannual	Official European Commission source for Common European Data Spaces, single-market data governance, cross-domain infrastructures, and interoperability specifications.
[Commission, 2026f]	cross_border_data_spaces	cross_border_data_spaces	official_primary	2026-05-22	semiannual	Official European Commission strategy source for single-market data, data sovereignty, common data spaces, and rights-preserving innovation.
[Consortium, 2023a]	agent_interoperability_standards	agent_interoperability_standards	international_standard	2026-05-22	annual	W3C Recommendation for Web of Things architecture, thing models, security considerations, interoperability, and application patterns.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Consortium, 2023c]	agent_interoperability_standards	agent_interoperability_standards	international_standard	2026-05-22	annual	W3C Recommendation for machine-readable thing descriptions, interaction affordances, metadata, security, and protocol bindings.
[Consortium, 2023b]	agent_interoperability_standards	agent_interoperability_standards	international_standard	2026-05-22	annual	W3C Recommendation for discovering Web of Things resources using directories, metadata, privacy, and security considerations.
[Initiative, 2026b]	agent_interoperability_standards	agent_interoperability_standards	open_standard	2026-05-22	semiannual	Official OpenAPI specification index for describing HTTP APIs, schemas, operations, errors, and contract validation.
[Consortium, 2025b]	agent_interoperability_standards	agent_interoperability_standards	international_standard	2026-05-22	annual	W3C Recommendation for verifiable credentials, issuers, holders, verifiers, security, privacy, internationalization, and accessibility considerations.
[Consortium, 2022]	agent_interoperability_standards	agent_interoperability_standards	international_standard	2026-05-22	annual	W3C Recommendation for decentralized identifiers, DID documents, verification methods, service endpoints, privacy, and security considerations.
[Force, 2022]	agent_interoperability_standards	agent_interoperability_standards	standard	2026-05-22	annual	IETF standard for HTTP semantics used to ground API contracts, methods, status codes, content negotiation, and safe integration language.
[Organization, 2026a]	workforce_governance	workforce_governance	official_primary	2026-05-22	semiannual	Official ILO topic page for AI and work, digital transformation, occupational impact, skills, safety, and social dialogue.
[Organization and Nations, 2024]	workforce_governance	workforce_governance	official_primary	2026-05-22	annual	Official ILO/UN publication on uneven AI adoption, labour-market exposure, global equity, fairness, and social justice.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Organization, 2019]	workforce_governance	workforce_governance	official_primary	2026-05-22	annual	Official ILO source for a human-centred future-of-work agenda, lifelong learning, labour guarantees, social protection, and decent work.
[Observatory, 2026a]	workforce_governance	workforce_governance	official_primary	2026-06-06	semiannual	Official OECD.AI source for AI, work, labour-market transitions, skills, productivity, workplace governance, and policy responses.
[Consortium, 2013b]	model_data_provenance	model_data_provenance	international_standard	2026-05-22	annual	W3C Recommendation overview for provenance interchange, entities, activities, agents, and provenance-family specifications.
[Consortium, 2013a]	model_data_provenance	model_data_provenance	international_standard	2026-05-22	annual	W3C Recommendation for the PROV ontology supporting machine-readable provenance relationships among entities, activities, agents, and roles.
[Consortium, 2024]	model_data_provenance	model_data_provenance	international_standard	2026-05-22	annual	W3C Recommendation for cataloging datasets and data services with metadata, distributions, provenance, access, and quality signals.
[Consortium, 2017]	model_data_provenance	model_data_provenance	international_standard	2026-05-22	annual	W3C Recommendation for publishing data with metadata, licenses, provenance, quality, versioning, identifiers, and machine-readable formats.
[of Standards and Technology, 2026h]	model_data_provenance	model_data_provenance	official_primary	2026-06-06	annual	Official NIST program source for big-data interoperability, reference architecture, data interfaces, vocabulary, and technology roadmap.
[DataCite, 2026]	model_data_provenance	model_data_provenance	research_standard	2026-05-22	annual	Official DataCite schema source for dataset citation metadata, persistent identifiers, creators, dates, relationships, and versioning.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[for Content Provenance and Authenticity, 2026]	model_data_provenance	model_data_provenance	technical_standard	2026-06-06	semiannual	C2PA specifications source for content credentials, provenance manifests, assertions, signing, verification, and media authenticity evidence.
[Initiative, 2026c]	accessibility_digital_inclusion	accessibility_digital_inclusion	technical_standard	2026-05-22	semiannual	W3C WAI overview for WCAG 2.0, 2.1, and 2.2 conformance, success criteria, and accessibility standard selection in digital curriculum artifacts.
[CAST, 2024]	accessibility_digital_inclusion	accessibility_digital_inclusion	inclusion_guidance	2026-05-22	annual	CAST UDL Guidelines 3.0 source for designing multiple means of engagement, representation, action, expression, and learner agency.
[of Justice, 2024]	accessibility_digital_inclusion	accessibility_digital_inclusion	official_primary	2026-05-22	quarterly	DOJ ADA Title II fact sheet for state and local government web and mobile app accessibility obligations, WCAG technical standard use, contractors, and compliance timing.
[Board, 2026]	human_rights_governance	rights_impact_privacy	official_primary	2026-05-22	semiannual	EDPB data-protection guide entry defining DPIA use for planned processing, high-risk processing, automated evaluation, sensitive data, and systematic monitoring.
[Board, 2018]	human_rights_governance	rights_impact_privacy	official_primary	2026-05-22	semiannual	EDPB list of endorsed WP29 GDPR guidelines, including DPIA guidance for processing likely to result in a high risk.
[OECD, 2015]	public_sector_agentic_ai	procurement_vendor_governance	official_primary	2026-05-22	annual	OECD public procurement legal instrument for transparency, integrity, access, risk management, accountability, evaluation, and supplier participation.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Partnership, 2026]	public_sector_agentic_ai	procurement_vendor_governance	technical_standard	2026-05-22	annual	International open data standard for publishing public contracting data and documents across planning, tender, award, contract, and implementation stages.
[of Standards and Technology, 2025d]	cyber_threat_intelligence	agent_incident_response	official_primary	2026-05-22	semiannual	NIST SP 800-61 Rev. 3 source for integrating incident response with risk management, preparation, detection, response, and recovery.
[for Cybersecurity, 2020]	agentic_ai_security	ai_red_team_assurance	official_primary	2026-05-22	annual	ENISA AI cybersecurity report mapping AI lifecycle assets, threat landscape, supply-chain concerns, security controls, and data-protection needs.
[of Standards and Technology, 2026g]	agentic_ai_security	ai_red_team_assurance	official_primary	2026-05-22	quarterly	NIST AI security and resilience research hub for secure-and-resilient AI trustworthiness, adversarial machine learning taxonomy, and mitigation work.
[of Standards and Technology, 2026d]	agentic_ai_governance	ai_red_team_assurance	official_primary	2026-05-22	quarterly	NIST AI Resource Center source for AI RMF operationalization, playbook resources, crosswalks, profiles, and testing, evaluation, verification, and validation support.
[OECD, 2017]	public_sector_agentic_ai	public_sector_transparency	official_primary	2026-05-22	annual	OECD open government legal instrument for transparency, integrity, accountability, stakeholder participation, civic space, and public-sector disclosure.
[Consortium, 2025a]	model_data_provenance	model_data_provenance	technical_standard	2026-05-22	semiannual	W3C Recommendation for data integrity proofs, proof sets, proof chains, verification methods, and transformed data protection in verifiable credentials.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Margaret Mitchell and Gebru, 2019]	model_data_provenance	model_card_reporting	scholarly	2026-05-22	annual	Scholarly source for documenting intended use, evaluation procedures, benchmarked performance, limitations, and model-release context.
[Timnit Gebru and Crawford, 2021]	model_data_provenance	dataset_documentation	scholarly	2026-05-22	annual	Scholarly source for dataset documentation covering motivation, composition, collection process, recommended uses, communication, transparency, and accountability.
[Service, 2025b]	public_sector_agentic_ai_gov	algorithmic_transparency_reporting	official_primary	2026-05-22	quarterly	Official UK hub for ATRS records, public-sector transparency expectations, mandatory-scope policy, template guidance, and publication support.
[Service, 2025a]	public_sector_agentic_ai_gov	algorithmic_transparency_reporting	official_primary	2026-05-22	quarterly	Official guidance for completing and publishing ATRS records, including public-sector template support and repository submission expectations.
[of Standards and Technology, 2024a]	agentic_ai_security	secure_release_change_control	official_primary	2026-05-22	semiannual	NIST SSDF Community Profile for AI model development, AI systems using models, AI system acquisition, and secure lifecycle practices.
[Board, 2017]	accessibility_digital_inclusion	ict_accessibility_procurement	official_primary	2026-05-22	semiannual	Official ICT accessibility standards for federal information and communication technology, including procurement, development, maintenance, use, exceptions, and documentation.
[of Standards and Technology, 2025a]	agentic_ai_security	assurance_evaluation_evidence	official_primary	2026-05-22	quarterly	NIST ARIA pilot report describing evaluation scenarios, model testing, red teaming, field testing, dialogue annotation, tester questionnaires, and measurement trees.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Archives and Administration, 2026a]	public_sector_agentic_ai	records_retention_auditability	official_primary	2026-05-22	quarterly	Official NARA inventory of current and planned AI use cases, including production, pilot, and planned AI applications tied to records, discovery, FOIA, and archival access.
[of the President, 2025a]	public_sector_agentic_ai	risk_exception_governance	official_primary	2026-05-22	quarterly	OMB memorandum for federal AI strategies, AI maturity, data traceability, continuous monitoring, governance, privacy, security, workforce, and public trust.
[of the President, 2025b]	procurement_vendor_governance	procurement_performance	official_primary	2026-05-22	quarterly	OMB memorandum for federal AI acquisition, product demonstrations, performance-based requirements, Quality Assurance Surveillance Plans, monitoring, and transparency requirements.
[of Standards and Technology, 2024e]	agentic_ai_governance	assurance_evaluation_evidence	primary	2026-06-11	semiannual	NIST AI 600-1 profile for generative AI risk management, risk framing, evaluation actions, misuse considerations, and AI RMF alignment.
[Cybersecurity and Agency, 2024a]	agentic_ai_governance	ai_red_team_assurance	official_primary	2026-05-22	semiannual	CISA guidance connecting AI red teaming to testing, evaluation, verification, and validation for security and safety assurance.
[Cybersecurity et al., 2025b]	model_data_provenance	model_data_provenance	official_primary	2026-06-11	semiannual	Joint official cybersecurity information sheet on best practices for securing data used to train and operate AI systems across the lifecycle.
[of Standards and Technology, 2026e]	ics_ot_defense	assurance_evaluation_evidence	primary	2026-05-22	quarterly	NIST concept note for a critical-infrastructure AI RMF profile covering AI-enabled IT, OT, and industrial-control environments.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[for Economic Co-operation and Development, 2025b]	public_sector_agentic_ai	public_sector_transparency	official_primary	2026-05-22	semiannual	OECD public-sector AI governance report framing enablers, guardrails, and engagement for trustworthy AI in government.
[Archives and Administration, 2025]	public_sector_agentic_ai	records_retention_auditability	official_primary	2026-05-22	semiannual	NARA plan for AI governance, public trust, audits, records-aware AI use, transparency, and compliance with federal AI policy.
[of Canada Secretariat, 2026a]	public_sector_agentic_ai	public_sector_agentic_ai	official_primary	2026-05-24	quarterly	Government of Canada guide for accountable public-sector use of agentic AI, including governance, risk, transparency, testing, monitoring, and human oversight considerations.
[of Canada Secretariat, 2026b]	rights_impact_privacy	rights_impact_privacy	official_primary	2026-05-24	quarterly	Government of Canada Algorithmic Impact Assessment tool for structured impact-level scoring, mitigation planning, and accountable review of automated decision systems.
[of Canada Secretariat, 2025]	public_sector_agentic_ai	public_sector_transparency	official_primary	2026-05-24	quarterly	Official announcement of Canada's federal AI register, used as a transparency anchor for AI use-case inventories and public-facing disclosure.
[of Canada, 2025]	public_sector_agentic_ai	workforce_governance	official_primary	2026-05-24	quarterly	Government of Canada AI Strategy priority-area page for public-service AI adoption, governance, people, public value, and responsible implementation.
[for Economic Co-operation and Development, 2026b]	agentic_ai_security	agent_incident_response	official_primary	2026-05-24	quarterly	OECD topic page on AI risks and incidents, including AI incident monitoring, hazard evidence, and the need for common incident reporting.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[for Economic Co-operation and Development, 2025a]	agentic_ai_security	agent_incident_response	official_primary	2026-05-24	quarterly	OECD policy paper proposing a common AI incident reporting framework for jurisdictions and sectors, including criteria for impact and risk characterization.
[Nations, 2024]	human_rights_governance	accessibility_digital_inclusion	official_primary	2026-05-24	semiannual	United Nations Global Digital Compact page and adopted compact context for inclusive, rights-based digital cooperation and global AI governance.
[of Standards and Technology, 2026i]	agentic_ai_governance	ai_red_team_assurance	official_primary	2026-05-24	quarterly	NIST Dioptra test platform for evaluating AI system risks, adversarial robustness, and measurement workflows in controlled settings.
[Cybersecurity et al., 2024]	agentic_ai_security	secure_release_change_control	official_primary	2026-05-24	semiannual	CISA joint guidance for deploying AI systems securely, used as a release/change-control anchor for AI-enabled services.
[Cybersecurity and Agency, 2025b]	ics_ot_defense	procurement_vendor_governance	official_primary	2026-05-24	semiannual	CISA Secure by Demand considerations for OT owners and operators selecting digital products, used for vendor-governance and procurement review.
[Cybersecurity et al., 2025a]	ics_ot_defense	records_retention_auditability	official_primary	2026-05-24	semiannual	CISA and partners' asset-inventory guidance for strengthening operational technology security and keeping OT records reviewable.
[Cybersecurity and Agency, 2025a]	ics_ot_defense	assurance_evaluation_evidence	official_primary	2026-05-24	semiannual	CISA guidance on creating and maintaining a definitive view of OT architecture, used as an assurance-evidence anchor for cyber-physical readiness.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[of Excellence, 2026]	human_rights_governance	human_rights_governance	official_primary	2026-05-22	semiannual	CCDCOE 2026 research reconceptualising cognitive warfare as a contest over the structures of interpretation and decision-making rather than information content; introduces systemic invariants and cognitive decoherence.
[Agency, 2024a]	agentic_ai_governance	assurance_evaluation_validation	official_primary	2026-05-22	semiannual	DARPA Intrinsic Cognitive Security (ICS) program applying probabilistic formal methods to guarantee mixed-reality system designs mitigate cognitive attacks; CAMP knowledgebase analog to MITRE CAPEC.
[Alliance, 2025a]	agentic_ai_security	agent_incident_response	official_primary	2026-05-22	quarterly	CSA Cognitive Degradation Resilience (CDR) framework defining a six-stage degradation cascade for agentic AI networks and seven QSAF-BC controls; treated as a defensive evidence-bounded governance anchor.
[Alliance, 2025b]	agentic_ai_security	ai_red_team_assurance	official_primary	2026-05-22	quarterly	CSA MAESTRO seven-layer threat-modeling framework for the full agentic AI stack from foundation model through agent ecosystem, including the vertical security/compliance layer.
[Mandel and Tetlock, 2018]	education_assessment	education_assessment	scholarly_peer_reviewed	2026-05-22	annual	Peer-reviewed Frontiers in Psychology analysis (NIH PMC) on correcting judgment in national security intelligence, identifying neglect of noise and unipolar treatment of bipolar bias in IC debiasing.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[arXiv preprint authors, 2025a]	agentic_ai_security	ai_red_team_assurance	scholarly_preprint	2026-05-22	quarterly	arXiv survey on agentic AI security providing a comprehensive threat taxonomy, defense catalog, evaluation review, and governance perspectives; vendor statistics within treated as ESTIMATE.
[Anthropic, 2024]	agent_interoperability_standards	agent_interoperability_standards	frontier_lab_research	2026-05-22	semiannual	Anthropic research guide establishing the canonical workflows-versus-agents taxonomy and composable agentic patterns (prompt chaining, routing, parallelization, orchestrator-workers, evaluator-optimizer).
[DeepMind and Research, 2026]	model_data_provenance	model_data_provenance	frontier_lab_research	2026-05-22	annual	Google DeepMind arXiv paper defining the epistemic AI agent and proposing demonstrable competence, falsifiability, virtuous behavior, provenance chains, verifier agents, and knowledge sanctuaries.
[Lee and Tiwari, 2024]	agentic_ai_security	agent_incident_response	scholarly_preprint	2026-05-22	annual	arXiv paper documenting self-replicating LLM-to-LLM prompt injection within multi-agent systems; used as a defensive, evidence-bounded counterintelligence anchor with LLM-tagging mitigation.
[arXiv preprint authors, 2025b]	agentic_ai_security	secure_release_change_control	scholarly_preprint	2026-05-22	annual	arXiv analysis framing prompt injection as structurally equivalent to dynamic code loading and arguing for dynamic, context-sensitive privilege management in agentic systems.
[Initiative), 2025]	agentic_ai_security	ai_red_team_assurance	official_primary	2026-05-22	quarterly	OWASP Agentic Security Initiative threat-model-based reference of emerging agentic AI threats and mitigations; standards-body guidance for defensive curriculum use.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Alliance, 2026]	agentic_ai_governance	procurement_vendor_governance	official_primary	2026-05-22	quarterly	CSA survey on securing autonomous AI agents quantifying the identity-governance gap; readiness percentages treated as ESTIMATE for curriculum discussion.
[Initiative, 2026a]	agentic_ai_governance	ai_red_team_assurance	official_primary	2026-05-22	quarterly	CSA research note on NIST AI agent red-teaming standards summarizing CAISI findings and recommended adversarial-ML testing protocols; reported success-rate figures treated as ESTIMATE.
[United Nations University, 2026]	human_rights_governance	human_rights_governance	official_primary	2026-05-22	semiannual	UNU Macau policy analysis arguing agentic AI requires boundaries before freedom — minimum necessary privilege, delimited scope, sandboxes, explicit permissions, and accountable oversight.
[of Standards and Technology, 2024b]	model_data_provenance	model_data_provenance	official_primary	2026-06-11	annual	NIST AI 100-4 report on reducing risks posed by synthetic content through digital content transparency, provenance, labeling, watermarking, detection, testing, auditing, and maintenance approaches.
[of Standards and Technology, 2024c]	ai_conformity_compliance	ai_conformity_compliance	official_primary	2026-06-06	annual	NIST AI 100-5 plan for global engagement on AI standards, used to ground standards coordination and cross-jurisdiction AI-governance discussions without claiming a single universal compliance regime.
[U.S. AI Safety Institute and Technology, 2024]	agentic_ai_governance	ai_red_team_assurance	official_draft	2026-06-06	quarterly	NIST AI 800-1 initial public draft on managing misuse risk for dual-use foundation models; used as draft official guidance, not as finalized regulation.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Group and Panel, 2026]	agentic_ai_governance	assurance_evaluation_evidence	scientific_synthesis	2026-06-12	annual	International AI Safety Report 2026 chaired by Yoshua Bengio with an international expert advisory panel; used as a synthesis source for advanced-AI safety evidence and uncertainty, not as a policy endorsement.
[Project, 2025c]	agent_interoperability	agent_standards	official_docs	primary	2026-06-11	quarterly	Official Model Context Protocol specification page for the 2025-06-18 version, grounding agent-tool interoperability language and protocol-boundary examples.
[Project, 2025b]	agentic_ai_security	secure_release_change_control	official_docs	primary	2026-06-11	quarterly	Official MCP security best practices page describing security considerations, attack vectors, and implementation practices for MCP deployments.
[Project, 2025a]	agent_interoperability	agent_standards	official_docs	primary	2026-06-06	quarterly	Official Agent2Agent (A2A) protocol documentation describing an open standard for AI agents to securely communicate, collaborate, and coordinate work.
[Centre and international partners, 2024]	agentic_ai_security	secure_release_change_control	official_docs	primary	2026-06-06	annual	NCSC Guidelines for secure AI system development for providers of systems that use AI, including systems built from scratch and systems built on top of third-party tools or services.
[MITRE, 2026d]	cyber_threat_intelligence	assurance_evaluation_evidence	research_standard	2026-06-06	quarterly	MITRE D3FEND knowledge base of cybersecurity countermeasure techniques and relationships to offen- sive/adversary techniques; used to ground defensive-control mapping without operationalizing attacks.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Open, 2022]	cyber_threat_intelligence	records_retention_auditability	technical_standard	2026-06-12	annual	OASIS Common Security Advisory Framework Version 2.0 standard for machine-readable vulnerability and remediation advisories, used to ground audit-ready incident and procurement evidence.
[Project, 2026a]	agentic_ai_security	model_data_provenance	security_standard	2026-06-06	quarterly	CycloneDX specification overview for bill-of-materials formats, used to ground component inventory, dependency provenance, and supplier evidence in agentic AI systems.
[SPDX Project, 2024]	model_data_provenance	model_data_provenance	technical_standard	2026-06-06	annual	SPDX 3.0.1 specification for creating software bills of materials and related machine-readable provenance records; used to ground model/data/software documentation evidence.
[of Standards and Technology, 2026j]	legal_oversight	records_retention_auditability	primary	2026-06-06	quarterly	NIST Open Security Controls Assessment Language project, used to ground machine-readable control catalogs, assessment evidence, and compliance traceability.
[chain Levels for Software Artifacts Project, 2026]	agentic_ai_security	secure_release_change_control	standard	2026-06-06	quarterly	SLSA specification for describing and incrementally improving software supply-chain security, used to ground artifact provenance and release-control claims.
[in-toto Project, 2026]	model_data_provenance	secure_release_change_control	standard	2026-06-06	quarterly	in-toto framework for securing software supply-chain integrity with verifiable metadata and attestations; used to ground release-chain evidence and provenance checks.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Project, 2026c]	agentic_ai_security	secure_release_change_control	standard	2026-06-06	quarterly	Sigstore documentation overview for software signing and transparency-log backed artifact verification, used to ground tamper-evident release and provenance evidence.
[Friston, 2010]	cognitive_active_inference	cognitive_active_inference	scholarly_peer_review	2026-06-08	annual	Karl Friston's flagship review introducing the free-energy principle, showing how a variational free-energy functional provides a tractable upper bound on surprise (negative log model evidence) that the brain minimizes through perception and action.
[Friston, 2017]	cognitive_active_inference	cognitive_active_inference	scholarly_peer_review	2026-06-08	annual	Formalizes active inference as a process theory in which belief updating proceeds by gradient descent on variational free energy and policies are selected by minimizing expected free energy over a Markov decision process generative model.
[Da Costa, 2020]	cognitive_active_inference	cognitive_active_inference	scholarly_peer_review	2026-06-08	annual	A mathematical synthesis of active inference over discrete (POMDP) state-spaces, consolidating the partially observable Markov decision process model used to specify perception, planning, and action selection in agentic systems.
[Parr, 2022]	cognitive_active_inference	cognitive_active_inference	scholarly_textbook	2026-06-08	annual	The open-access MIT Press monograph giving the book-length, chapter-organized foundational treatment of active inference, from the free-energy principle to discrete and continuous generative models and their behavioral implications.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Yao, 2023a]	agentic_ai_governance	agentic_ai_governance	scholarly_preprint	2026-06-08	annual	Introduces the interleaved reason-then-act loop in which an LLM alternates verbal reasoning traces with tool/environment actions, grounding the reason-act/tool-use pattern at the core of modern agent design.
[Shinn, 2023]	agentic_ai_governance	agentic_ai_governance	scholarly_preprint	2026-06-08	annual	Proposes agents that verbally reflect on task feedback and store reflections in episodic memory to improve on later trials, grounding the self-reflection and stop-condition pattern for iterative agents.
[Park, 2023]	agentic_ai_governance	agentic_ai_governance	scholarly_peer_review	2026-06-08	annual	Demonstrates a multi-agent sandbox of twenty-five LLM agents whose memory-stream, reflection, and planning architecture produces believable emergent social behavior, grounding the memory/planning/multi-agent-simulation pattern.
[Wei, 2022]	agentic_ai_governance	agentic_ai_governance	scholarly_preprint	2026-06-08	annual	Shows that prompting an LLM to emit intermediate reasoning steps markedly improves complex reasoning, establishing the reasoning-decomposition pattern that underlies agent planning and ReAct-style traces.
[Schick, 2023]	agentic_ai_governance	agentic_ai_governance	scholarly_preprint	2026-06-08	annual	Shows an LLM self-supervising when and how to call external APIs (calculator, search, QA, translation, calendar), grounding the tool-use / API-calling pattern for agents.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Wooldridge, 1995]	agentic_ai_governance	agentic_ai_governance	scholarly_peer_reviewed	2026-06-08	annual	Foundational survey dividing agent research into theory, architectures, and languages, providing the canonical agent definition and multi-agent-systems vocabulary that predates the LLM era.
[Wooldridge, 2009]	agentic_ai_governance	agentic_ai_governance	scholarly_textbook	2026-06-08	annual	Standard graduate textbook on multi-agent systems covering coordination, negotiation, voting, and auctions, grounding the multi-agent-coordination vocabulary used in agentic governance.
[Burkett, 2013]	counterintelligence_source_integrity	counterintelligence_source_integrity	official_primary	2026-06-08	annual	A CIA Studies in Intelligence analyst essay arguing that the traditional MICE recruitment-motivation model (Money, Ideology, Compromise, Ego) is better understood through Cialdini's influence principles reframed as RASCLS (Reciprocation, Authority, Scarcity, Commitment/Consistency, Liking, Social Proof), grounding the historical and conceptual lineage of HUMINT recruitment frameworks.
[Meissner, 2017]	counterintelligence_source_integrity	counterintelligence_source_integrity	scholarly_peer_reviewed	2026-06-08	annual	A peer-reviewed synthesis of the HIG-funded research program summarizing scores of empirical studies showing that rapport-based, non-coercive interviewing reliably outperforms accusatorial or coercive methods for eliciting accurate information, establishing the evidence base for rights-respecting elicitation.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Brimbal, 2020]	counterintelligence_source_integrity	counterintelligence_source_integrity	scholarly_integrity_review	2026-06-08	annual	An Oxford volume chapter reviewing the empirical and ethical case for rapport- and trust-based interrogation as an alternative to customary coercive practices, grounding the contrast between rapport-based and coercive elicitation and the ethics/consent governance that distinguishes them.
[Nunan, 2020]	counterintelligence_source_integrity	counterintelligence_source_integrity	scholarly_integrity_review	2026-06-08	annual	A peer-reviewed study of UK police source handlers' lived perceptions of rapport during interactions with covert human intelligence sources, grounding how rapport functions in real source-handler tradecraft and the governance of HUMINT/CHIS relationships.
[Kelly, 2013]	counterintelligence_source_integrity	counterintelligence_source_integrity	scholarly_integrity_review	2026-06-08	annual	A peer-reviewed taxonomy organizing interrogation into macro-level approaches, six meso-level domains (rapport/relationship building, context manipulation, emotion provocation, confrontation/competition, collaboration, presentation of evidence), and micro-level techniques, providing a study-grounded vocabulary for analyzing elicitation methods rather than an operational manual.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Pherson, 2014a]	analytic_tradecraft	analytic_tradecraft	scholarly_textbook	2026-06-08	annual	The standard practitioner catalogue of fifty-five structured analytic techniques (e.g., Analysis of Competing Hypotheses, Key Assumptions Check, Devil's Advocacy) used to counter cognitive bias in intelligence analysis.
[of Standards and , NIST]	cyber_threat_intelligence	cyber_threat_intelligence	technical_standard	2026-06-08	annual	The U.S. federal standard specifying the AES block cipher, the canonical symmetric algorithm providing data confidentiality.
[of Standards and , NIST]	cyber_threat_intelligence	cyber_threat_intelligence	technical_standard	2026-06-08	annual	The U.S. federal standard specifying approved digital-signature algorithms (e.g., ECDSA, EdDSA, RSA) used to authenticate signatories and detect unauthorized data modification.
[of Standards and , NIST]	cyber_threat_intelligence	cyber_threat_intelligence	technical_standard	2026-06-08	annual	The U.S. federal standard specifying the SHA family of cryptographic hash functions used to produce fixed-length digests for data-integrity verification.
[, NIST]	cyber_threat_intelligence	cyber_threat_intelligence	technical_standard	2026-06-08	annual	NIST's general guidance on cryptographic key management, covering key types, cryptoperiods, and lifecycle governance across the full key life.
[McGuire, 1961]	cognitive_influence_security	cognitive_influence_security	scholarly_peer_reviewed	2026-06-08	annual	The founding inoculation-theory experiment, showing that pre-exposing people to weakened counterarguments (refutational pre-bunking) builds resistance to later persuasion better than passive supportive defenses — the medical-vaccination analogy that grounds modern prebunking research.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Mahima Pushkarna and Kjartansson, 2022]	model_data_provenance	dataset_documentation	scholarly_peer_review	2026-06-09	annual	ACM FAccT paper introducing Data Cards as structured, purposeful, human-centered summaries of dataset facts needed by stakeholders across a dataset lifecycle for responsible AI development.
[Christopher L. Buckley and Seth, 2017]	cognitive_active_inference	cognitive_active_inference	scholarly_preprint	2026-06-10	annual	arXiv scholarly review that works through the free energy principle and active inference mathematically, including an agent-based model and the assumptions needed for the formal result.
[Melissa L. Rethlefsen and the PRISMA-S Group, 2021]	source_construction_reporting	reporting_construction_reporting	scholarly_peer_review	2026-06-10	annual	Systematic Reviews article introducing the PRISMA-S extension, a 16-item checklist for transparent, reproducible reporting of search methods in evidence syntheses.
[Kai Greshake and Fritz, 2023]	agentic_ai_security	agentic_ai_security	scholarly_preprint	2026-06-10	annual	arXiv security paper showing that malicious third-party content retrieved by LLM-integrated applications can indirectly inject instructions and compromise real-world application behavior.
[of Standards and Technology, 2026b]	agentic_ai_governance	assurance_evaluation_guidance	official_draft	2026-06-11	quarterly	NIST AI 800-2 initial public draft provides voluntary practices for automated benchmark evaluations of language models and AI agent systems.
[for Economic Co-operation and Development, 2026a]	agentic_ai_governance	agent_interoperability_standards	official_policy_analysis	2026-06-11	semiannual	OECD AI paper clarifying the agentic AI landscape and conceptual foundations by comparing definitions and mapping shared features to the OECD AI system definition.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Agency, 2026i]	agentic_ai_security	secure_release_change_control	official_primary	2026-06-11	quarterly	NSA cybersecurity information sheet on MCP security design considerations for organizations adopting MCP-based AI toolchains.
[Jon Roozenbeek and Lewandowsky, 2022]	cognitive_influence_security	cognitive_resilience_evidence	scholarly_peer_reviewed	2026-06-11	annual	Science Advances article showing that psychological inoculation campaigns on social media can improve misinformation resilience at scale under measured study conditions.
[for the Study of Intelligence, 2002]	analytic_tradecraft	analytic_tradecraft_evidence	official_primary	2026-06-11	annual	Official CIA Center for the Study of Intelligence essay on Kent's professionalization of intelligence analysis and analytic standards.
[for the Study of Intelligence, 1994]	analytic_tradecraft	analytic_tradecraft_evidence	official_primary	2026-06-11	annual	Official CIA CSI republication of Kent's final essay on analyst-policy relations, warning, intention, and communication boundaries.
[Wohlstetter, 1962]	analytic_tradecraft	warning_intelligence	scholarly_publisher_record	2026-06-11	annual	Publisher record for Wohlstetter's classic warning-intelligence study of signal, noise, and surprise before Pearl Harbor.
[Grabo, 1972]	analytic_tradecraft	warning_intelligence	official_declassified_primary	2026-06-11	annual	CIA Reading Room declassified warning-intelligence handbook volume used for indications-and-warning concepts.
[Congress, 2004]	analytic_tradecraft	intelligence_failure_postmortem	official_statute	2026-06-11	biennial	Official GovInfo public law record establishing post-9/11 intelligence reform requirements including alternative analysis and analytic integrity provisions.
[on Terrorist Attacks Upon the United States, 2004]	analytic_tradecraft	intelligence_failure_postmortem	official_report	2026-06-11	biennial	Official commission report used for postmortem context on warning, information sharing, imagination, and reform pressures after September 11, 2001.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005]	analytic_tradecraft	intelligence_failure_postmortem	official_report	2026-06-11	biennial	Official WMD Commission report used for Iraq WMD analytic-failure context, assumptions-versus-evidence boundaries, and reform pressure.
[Transformation, 2017]	analytic_tradecraft	analytic_tradecraft_method	official_alliance_guidance	2026-06-11	annual	Official NATO handbook presenting alternative-analysis techniques and facilitation practices for analytic teams.
[Bruce, 2016]	analytic_tradecraft	sat_evaluation_evidence	policy_research_report	2026-06-15	annual	RAND report on the difficulty of measuring SAT value and the need for systematic evaluation before strong effectiveness claims.
[Alexandru Marcoci and Jonas, 2019]	analytic_tradecraft	sat_evaluation_evidence	scholarly_peer_reviewed	2026-06-11	annual	Peer-reviewed study showing poor individual reliability but stronger aggregated reliability when raters apply tradecraft standards to intelligence reports.
[Barnes and Mandel, 2014]	analytic_tradecraft	forecasting_calibration_evidence	scholarly_peer_reviewed	2026-06-11	annual	Peer-reviewed PNAS study of strategic-intelligence forecast accuracy, calibration, discrimination, and probability-language behavior.
[Ard, 2024]	analytic_tradecraft	sat_evaluation_evidence	scholarly_peer_reviewed	2026-06-15	annual	Peer-reviewed critique arguing that SAT evidence is thinner than many tradecraft claims imply and that SATs should not be treated as universal bias remedies.
[Jennifer Stromer-Galley and colleagues, 2020]	analytic_tradecraft	sat_evaluation_evidence	scholarly_repository_record	2026-06-11	annual	Scholarly record and abstract for an experimental comparison of flexible SAT support and structured/no-SAT conditions for reasoning quality.
[Betts, 1978]	analytic_tradecraft	intelligence_failure_postmortem	scholarly_peer_reviewed	2026-06-11	annual	Classic peer-reviewed failure-theory article on the interaction of analysis, decision, leadership psychology, and policy uptake.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Jervis, 2022]	analytic_tradecraft	intelligence_failure_postmortems	scholarly_peer_reviewed	2026-06-11	annual	PNAS perspective on intelligence-policy friction and the limits of postmortem explanations of intelligence failure.
[Wirtz, 2023]	analytic_tradecraft	intelligence_failure_postmortems	scholarly_peer_reviewed	2026-06-11	annual	Peer-reviewed discussion revisiting intelligence-failure inevitability in light of collection, analysis, reform, and policy factors.
[Central Intelligence Agency, 1993]	analytic_tradecraft	analytic_uncertainty_vocabulary	official_primary	2026-06-14	annual	CIA/CSI source for disciplined probability language and the review boundary between estimative wording, evidence, and numeric interpretation.
[Central Intelligence Agency, 1970s]	analytic_tradecraft	analytic_uncertainty_vocabulary	official_primary	2026-06-14	annual	CIA/CSI historical source for uncertainty vocabulary, disagreement, and estimative communication problems.
[Central Intelligence Agency, 2018b]	analytic_tradecraft	analytic_method_design	official_primary	2026-06-14	annual	CIA/CSI analytic-methods source for decomposing analysis variables and avoiding one-piece judgment claims.
[Johnston, 2005]	analytic_tradecraft	intelligence_profession_literature	official_primary	2026-06-15	annual	CIA/CSI professional-literature monograph on analytic institutions, incentives, training, and cultural constraints.
[Central Intelligence Agency, 1955]	analytic_tradecraft	intelligence_profession_literature	official_primary	2026-06-14	annual	Classic CIA/CSI source for why intelligence practice needs a professional literature and reviewable doctrine.
[Central Intelligence Agency, 2025b]	analytic_tradecraft	intelligence_writing_review	official_primary	2026-06-14	annual	CIA/CSI writing-guide source for public professional writing norms, review boundaries, and publication discipline.
[Central Intelligence Agency, 2025a]	analytic_tradecraft	analytic_epistemology	official_primary	2026-06-14	annual	CIA/CSI source for epistemic framing, objectivity, knowledge claims, and analytic habits of thinking.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Central Intelligence Agency, 2023]	analytic_tradecraft	analytic_production_workflow	official_primary	2026-06-14	annual	CIA/CSI source for team-based analytic production, iteration, and experimentation boundaries.
[Central Intelligence Agency, 2018c]	analytic_tradecraft	intelligence_failure_post-mortem	official_primary	2026-06-14	annual	CIA/CSI source for reliability, intelligence failure, feedback, and institutional learning cycles.
[Central Intelligence Agency, 2018f]	analytic_tradecraft	intelligence_failure_post-mortem	official_primary	2026-06-14	annual	CIA/CSI source for analyst error, limits, and institutional conditions around analytic failure.
[Central Intelligence Agency, 2019]	agentic_ai_governance	ai_enabled_analysis_boundary	official_primary	2026-06-14	annual	CIA/CSI source for future analytic work, data volume, automation, and human analytic structure.
[Central Intelligence Agency, 1999]	analytic_tradecraft	analytic_cognition_and_bias	official_primary	2026-06-14	annual	CIA/CSI public PDF of Richards Heuer's work on cognition, bias, evidence evaluation, and analytic judgment.
[Central Intelligence Agency, 1994]	historical_declassified_lessons	declassified_analytic_history	official_primary	2026-06-14	annual	CIA/CSI historical professional source for estimative practice, institutional review, and the Board of National Estimates.
[Central Intelligence Agency, 2020]	agentic_ai_governance	ai_enabled_analysis_boundary	official_primary	2026-06-14	annual	CIA/CSI article on an AI-enabled analytic experiment, used as bounded professional context for AI-assisted analysis.
[Central Intelligence Agency, 2018a]	analytic_tradecraft	analytic_cognition_and_bias	official_primary	2026-06-14	annual	CIA/CSI article supporting humility, uncertainty, and limits in analytic judgment.
[Central Intelligence Agency, 2021a]	analytic_tradecraft	analytic_method_design	official_primary	2026-06-14	annual	CIA/CSI article on foundational elements of intelligence analysis and disciplined analytic practice.
[Central Intelligence Agency, 2018e]	analytic_tradecraft	analytic_uncertainty_language	official_primary	2026-06-14	annual	CIA/CSI review source for uncertainty, probability expression, and the limits of confident prediction.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Central Intelligence Agency, 2005a]	historical_declassified	intelligence_profession	official_primary	2026-06-14	annual	CIA/CSI reflection on Studies in Intelligence as an official professional literature venue.
[Central Intelligence Agency, 2018d]	analytic_tradecraft	intelligence_writing_and_review	official_primary	2026-06-14	annual	CIA/CSI source connecting cognitive science, analytic writing, and intelligence-analysis communication.
[Central Intelligence Agency, 2005b]	analytic_tradecraft	analytic_method_design	official_primary	2026-06-14	annual	CIA/CSI source on analytic-method evaluation, evidence standards, and institutional method development.
[Central Intelligence Agency, 2006]	analytic_tradecraft	intelligence_profession	official_primary	2026-06-14	annual	CIA/CSI article for defining intelligence analysis around uncertainty rather than undifferentiated information processing.
[Central Intelligence Agency, 1998]	historical_declassified	declassified_analytic_digest	official_primary	2026-06-14	annual	CIA/CSI declassified historical source for analyst-policy boundary lessons and historical interpretation limits.
[Central Intelligence Agency, 2021b]	analytic_tradecraft	analytic_uncertainty_language	official_primary	2026-06-14	annual	CIA/CSI review source for uncertainty-management literature and analytic decision support.
[Central Intelligence Agency, 2017]	analytic_tradecraft	forecasting_calibration_evidence	official_primary	2026-06-14	annual	CIA/CSI source for prediction limits, forecasting caution, and analytic improvement boundaries.
[Central Intelligence Agency, 2026]	agentic_ai_governance	ai_enabled_analysis_drafting	official_primary	2026-06-14	annual	CIA/CSI 2026 article for AI-era espionage context, source skepticism, and human-review boundaries.
[of the Director of National Intelligence, 2026a]	governed_intelligence_cycle	current_threat_baseline	official_primary	2026-06-14	annual	ODNI unclassified annual threat assessment used as current public threat-context baseline, not as operational guidance.
[of the Director of National Intelligence, 2013a]	analytic_tradecraft	analytic_outreach_governance	official_primary	2026-06-14	annual	ODNI directive for analytic outreach, outside expertise, risk management, and citation of outreach insights.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[of the Director of National Intelligence, 2008]	governed_intelligence_activities	national_intelligence_council	official_primary	2026-06-14	annual	ODNI directive describing the National Intelligence Council and national intelligence production responsibilities.
[of the Director of National Intelligence, 2017b]	analytic_standards	analytic_product_dissemination	official_primary	2026-06-14	annual	ODNI directive for customer utility, analytic standards, tearlines, discoverability, and transparent products.
[of the Director of National Intelligence, 2012]	tearlines_and_releasability	foreign_disclosure_governance	official_primary	2026-06-14	annual	ODNI directive for tearlines and broader dissemination while protecting sources and methods.
[of the Director of National Intelligence, 2013b]	legal_oversight	foreign_disclosure_governance	official_primary	2026-06-14	annual	ODNI directive for foreign disclosure and release governance, marking, records, and release authority.
[of the Director of National Intelligence, 2024a]	governed_intelligence_activities	intelligence_diplomacy_synchronization	official_primary	2026-06-14	annual	ODNI directive for intelligence diplomacy, synchronization, and foreign-policy support boundaries.
[of the Director of National Intelligence, 2024b]	governed_intelligence_activities	non_state_engagement	official_primary	2026-06-14	annual	ODNI directive for non-state entity engagement, analytic outreach, privacy/civil-liberties, and no-tasking boundaries.
[of the Director of National Intelligence, 2024c]	legal_oversight	ic_information_environment_risk	official_primary	2026-06-14	annual	ODNI directive for risk management in the IC information environment.
[of the Director of National Intelligence, 2013f]	governed_intelligence_activities	integrated_mission_management	official_primary	2026-06-14	annual	ODNI directive for integrated mission management and IC mission alignment.
[of the Director of National Intelligence, 2017a]	governed_intelligence_activities	ic_information_environment_risk	official_primary	2026-06-14	annual	ODNI directive for the IC information environment, discovery, retrieval, sharing, and safeguarding.
[of the Director of National Intelligence, 2022]	financial_economic_security	economic_security_review	official_primary	2026-06-14	annual	ODNI directive for intelligence support to CFIUS threat analysis, economic-security review, and covered transactions.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[of the Director of National Intelligence, 2013d]	cyber_threat_intelligence	supply_chain_risk_governance	official_primary	2026-06-14	annual	ODNI directive for IC supply-chain risk management across mission-critical products, materials, and services.
[of the Director of National Intelligence, 2013c]	legal_oversight	classification_marking_governance	official_primary	2026-06-14	annual	ODNI directive for classification and control markings, including release and foreign-disclosure marking relationships.
[of the Director of National Intelligence, 2013e]	counterintelligence_program_governance	counterintelligence_program_governance	official_primary	2026-06-14	annual	ODNI directive establishing a baseline for counterintelligence programs across the IC.
[Intelligence.gov, 2026e]	governed_intelligence	ic_public_transparency	official_primary	2026-06-14	quarterly	Intelligence.gov public mission page describing the IC mission, customers, and values at a high level.
[Intelligence.gov, 2026b]	legal_oversight	ic_public_transparency	official_primary	2026-06-14	quarterly	Intelligence.gov public values page describing IC accountability, lawfulness, oversight, and civil liberties framing.
[Intelligence.gov, 2026f]	legal_oversight	ic_public_transparency	official_primary	2026-06-14	quarterly	Intelligence.gov public values page describing transparency principles, public understanding, and protection of sources and methods.
[Intelligence.gov, 2026a]	governed_intelligence	ic_public_transparency	official_primary	2026-06-14	quarterly	Intelligence.gov public page explaining the site as an IC transparency platform and public front door.
[Intelligence.gov, 2026c]	governed_intelligence	ic_public_transparency	official_primary	2026-06-14	quarterly	Intelligence.gov public values page describing collaboration across IC elements and external partners.
[Intelligence.gov, 2026d]	agentic_ai_governance	ic_public_transparency	official_primary	2026-06-14	quarterly	Intelligence.gov public values page describing innovation as more than technology and tying it to mission needs.
[Agency, 2024b]	osint_geoint	defense_osint_governance	official_primary	2026-06-14	annual	DIA strategy for professionalizing and unifying Defense OSINT collection and reporting in public governance terms.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Agency, 2015]	analytic_tradecraft	intelligence_writing_publication_review	official_primary	2026-06-14	annual	DIA public FOIA release for intelligence-production style, terminology, formatting, and writing consistency.
[Agency, 2014]	legal_oversight	rights_impact_privacy	official_primary	2026-06-14	annual	DIA public instruction for privacy and civil-liberties responsibilities, complaints, records, and safeguards.
[Agency, 2026f]	cyber_threat_intelligence	cyber_defense_guidance_publication	official_primary	2026-06-14	quarterly	NSA public index for cybersecurity advisories, information sheets, technical reports, and operational risk notices.
[Agency, 2026d]	governed_intelligence_ic_cyber	public_transparency	official_primary	2026-06-14	quarterly	NSA public mission page for SIGINT and cybersecurity mission context.
[Agency, 2026e]	agentic_ai_governance	agentic_ai_security_guidance_publication	official_primary	2026-06-14	quarterly	NSA public release announcing joint guidance on careful adoption of agentic AI services.
[Agency, 2017b]	osint_geoint	geoint_professional_doctrine	official_primary	2026-06-14	annual	NGA doctrine source for GEOINT definitions, mission context, and professional geospatial intelligence framing.
[Agency, 2021]	osint_geoint	geoint_data_governance	official_primary	2026-06-14	annual	NGA public release on data strategy, geospatial data management, and digital transformance in GEOINT.
[of Investigation, 2026]	counterintelligence_source_protection	counterintelligence_program_guidance	official_primary	2026-06-14	quarterly	FBI public counterintelligence page describing defensive goals and protection of IC secrets, critical assets, and sensitive information.
[Office, 2026b]	historical_declassified_publication	declassified_reconnaissance_history	official_history	2026-06-14	annual	NRO public history page describing the Center for the Study of National Reconnaissance and declassified history resources.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Dylan and Stivang, 2025]	agentic_ai_governance	ai_enabled_analysis_boundary	boundary	peer_reviewed	2026-06-15	annual	Peer-reviewed Intelligence and National Security article on emerging technologies and national security intelligence, used to frame AI and data-system effects as medium-term intelligence-work pressures requiring analytic governance.
[Caballero and Jenkins, 2024]	agentic_ai_governance	ai_enabled_analysis_boundary	boundary	preprint	2026-06-15	semiannual	arXiv preprint on LLMs in national-security applications, useful for classroom risk framing because it explicitly treats LLMs as support tools needing safeguards rather than strategic decision-makers.
[Mikhailov, 2023]	agentic_ai_governance	ai_enabled_analysis_boundary	boundary	preprint	2026-06-15	semiannual	arXiv preprint on LLM-driven AI integration in national-security strategy, encoded with a narrow claim scope because it is useful as a strategic-policy framing source rather than as empirical validation.
[Revanth Gangi Reddy and Ji, 2023]	analytic_tradecraft	ai_enabled_analysis_boundary	boundary	preprint	2026-06-15	semiannual	SmartBook preprint describing AI-assisted situation-report generation for intelligence analysts, including source grounding, analyst preferences, and evaluation caveats relevant to generated-product review.
[et al., 2024a]	agentic_ai_governance	ai_enabled_analysis_boundary	boundary	preprint	2026-06-15	semiannual	arXiv HTML source on foundation models and covert proliferation of military ISTAR capabilities, routed as a risk-boundary source for synthetic and defensive education.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[et al., 2023a]	cognitive_influence_synthetic	synthetic_media_provenance	scholarly_preprint	2026-06-15	semiannual	arXiv survey-style source on synthetic realities and AI-generated media risk, used for provenance, detection-limit, and public-trust framing in cognitive-security lessons.
[et al., 2018]	agentic_ai_governance	ai_red_team_assurance	scholarly_report	2026-06-15	annual	Foundational public report on malicious uses of AI, encoded for defensive taxonomy, safe-substitution, and governance framing in synthetic classroom work.
[for Security and Technology, 2022]	cyber_threat_intelligence	ai_red_team_assurance	public_domain_primary	2026-06-15	annual	CSET policy-research source on adversarial machine learning and cybersecurity, used to connect AI model robustness, defensive assurance, and cyber threat-intelligence review.
[Taddeo and Floridi, 2018]	cyber_threat_intelligence	cyber_threat_intelligence	scholarly_commentary	2026-06-15	annual	Nature Comment article arguing for AI-cyber governance before escalation risks intensify, useful for high-level cyber policy and non-escalatory classroom framing.
[Project and Institute, 2024]	agentic_ai_governance	ai_enabled_analysis_publication	public_domain_primary	2026-06-15	annual	SCSP/ASPI public report on AI and human-machine teaming for intelligence analysis, routed for governance, training, and analytic-workflow boundary discussion.
[McMahon, 2024]	analytic_tradecraft	analytic_tradecraft_evidence	public_domain_primary	2026-06-15	annual	Belfer Center Intelligence Project report on how AI tools interact with analytic tradecraft standards, especially source distinction, alternatives, uncertainty, and analyst ownership.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[et al., 2019]	analytic_tradecraft	sat_evaluation_evidence	scholarly_peer_reviewed	2026-06-15	annual	Applied Cognitive Psychology article on Analysis of Competing Hypotheses in intelligence analysis, routed as empirical/SAT evidence with explicit limitations.
[et al., 2024b]	analytic_tradecraft	sat_evaluation_evidence	scholarly_peer_reviewed	2026-06-15	annual	Cognitive Research article on how task structure affects confirmation bias and alternative hypotheses, useful for designing negative controls around ACH and SAT exercises.
[The White House, 1988]	collection_management	opsec_doctrine_governance	official_primary	2026-06-15	biennial	National Security Decision Directive 298 establishing national operations security program policy, used as public historical doctrine context for defensive OPSEC governance.
[Wardle and Derakhshan, 2017]	cognitive_influence_security	cognitive_influence_security	public_domain_primary	2026-06-15	annual	Council of Europe report providing an interdisciplinary framework for information disorder, routed as terminology and source-provenance support for defensive cognitive-security lessons.
[Deng and UNIDIR, 2023]	agentic_ai_governance	model_data_provenance	public_domain_primary	2026-06-15	annual	UNIDIR primer on synthetic data for artificial intelligence and autonomous systems, used for source-quality and risk caveats around synthetic fixtures and military AI governance.
[for Strategic and Studies, 2022]	cognitive_influence_security	synthetic_media_provenance	public_domain_primary	2026-06-15	annual	CSIS public analysis on deepfake risk as a policy and security concern, routed to synthetic-media provenance and cognitive-security safeguards.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[National Security Agency et al., 2023]	cognitive_influence_security	synthetic_media_provenance	official_primary	2026-06-15	semiannual	Joint Cybersecurity Information Sheet on contextualizing deepfake threats, routed as official defensive guidance for provenance and synthetic-media risk review.
[Agency, 2017a]	cyber_threat_intelligence	cyber_threat_intelligence	official_primary	2026-06-15	annual	DARPA public program page for Active Social Engineering Defense, used as official defensive context for social-engineering resilience and automation-risk caveats.
[et al., 2015]	cognitive_active_inference	cognitive_active_inference	scholarly_peer_reviewed	2026-06-15	annual	PubMed-indexed active-inference source on epistemic value, routed as theory support for bounded analogies in the cognitive-active-inference profile.
[et al., 2017]	cognitive_active_inference	cognitive_active_inference	scholarly_peer_reviewed	2026-06-15	annual	Open-access PMC article on uncertainty, epistemics, and active inference, encoded for theory boundaries and claim-calibration around active-inference analogies.
[et al., 2022]	cognitive_active_inference	cognitive_active_inference	scholarly_peer_reviewed	2026-06-15	annual	Open-access tutorial on active inference and empirical-data applications, routed as a learner-facing formal-method source for bounded AGEINT analogies.
[et al., 2021a]	cognitive_active_inference	cognitive_active_inference	scholarly_preprint	2026-06-15	annual	Zenodo-hosted scholarly source on active inference in modeling conflict, used only for bounded theory-to-scenario analogies and caveated simulation discussion.
[Kozera, 2020]	osint_geoint	osint_geoint	scholarly_peer_reviewed	2026-06-15	annual	Security and Defence article on identifying and tracking military and security personnel through fitness-app data, routed as a privacy and source-minimization warning.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[et al., 2025b]	cyber_threat_intelligence	red_team_assurance	scholarly_peer_reviewed	2026-06-15	annual	Journal article reviewing adversarial machine learning in cybersecurity, encoded as supplemental scholarly support for defensive AI red-team assurance.
[et al., 2023b]	cognitive_influence_security	cognitive_influence_scholarly	scholarly_peer_reviewed	2026-06-15	annual	Open-access Safety and Security article on AI challenges to cognitive security and safety, routed as bounded cognitive-security risk context.
[Deppe and Schaal, 2024]	cognitive_influence_security	cognitive_influence_scholarly	scholarly_peer_reviewed	2026-06-15	annual	Open-access PMC article on a NATO ACT cognitive-warfare concept, routed for conceptual and governance framing with explicit evidence-bounded limits.
[Terp and Breuer, 2022]	cognitive_influence_security	cognitive_influence_scholarly	scholarly_peer_reviewed	2026-06-15	annual	IEEE source on the DISARM framework for disinformation and influence operations, used for defensive taxonomy and reviewable incident mapping.
[et al., 2024c]	cognitive_influence_security	cognitive_influence_scholarly	scholarly_peer_reviewed	2026-06-15	annual	IEEE article on large language models and disinformation, routed as risk-and-defense context with explicit no-generation and no-campaign boundaries.
[et al., 2025c]	cognitive_influence_security	cognitive_influence_scholarly	scholarly_peer_reviewed	2026-06-15	annual	Open-access PMC article on LLM-generated election disinformation, routed as public-impact evidence for defensive cognitive-security education.
[et al., 2023c]	cognitive_influence_security	cognitive_influence_scholarly	scholarly_peer_reviewed	2026-06-15	annual	ACL EMNLP paper on using large language models for disinformation detection, routed as defensive method evidence with explicit reliability and rights caveats.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Farid and Bohacek, 2022]	cognitive_influence_security	synthetic_media_provenance	scholarly_peer_review	2026-06-15	annual	Open-access PMC article on protecting world leaders against deepfakes, routed as identity-integrity and provenance-risk support for defensive education.
[et al., 2020]	cognitive_influence_security	cognitive_influence_security	scholarly_peer_review	2026-06-15	annual	Open-access PMC article on human cognition in social-engineering cyberattacks, routed as defensive awareness and cognitive-security evidence with operational details excluded.
[et al., 2021b]	analytic_tradecraft	analytic_cognition_and_bias	scholarly_peer_review	2026-06-15	annual	Open-access PMC article on situation awareness in intelligence scenarios, useful for analytic-cognition lessons and scenario-review vocabulary.
[et al., 2024d]	agentic_ai_governance	agent_incident_response	scholarly_preprint	2026-06-15	semiannual	arXiv preprint on AI emergency preparedness, routed to agent incident-response and publication-readiness caveats for tabletop exercises.
[et al., 2025a]	legal_oversight	agent_incident_response	scholarly_preprint	2026-06-15	semiannual	arXiv HTML source on AI incident regimes, routed as comparative governance context for incident reporting, risk exceptions, and assurance evidence.
[Cooper, 2005]	analytic_tradecraft	analytic_tradecraft_primer	official_primary	2026-06-15	annual	CIA Center for the Study of Intelligence monograph on analytic pathologies, self-correction, and intelligence-process reform.
[Janis, 1982]	analytic_tradecraft	analytic_cognition_and_bias	scholarly_book_meta	2026-06-15	annual	Scholarly book record for Janis's groupthink model used as classic context for dissent, alternatives, and group-decision failure claims.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Coulthart, 2016]	analytic_tradecraft	sat_evaluation_evidence	scholarly_peer_reviewed	2026-06-15	annual	Peer-reviewed study of why analysts use SATs, supporting adoption, training, and organizational-context claims rather than universal efficacy claims.
[Coulthart, 2017]	analytic_tradecraft	sat_evaluation_evidence	scholarly_peer_reviewed	2026-06-15	annual	Peer-reviewed evaluation of core SATs used to qualify claims about where specific techniques may or may not have evidence support.
[Tetlock, 2018]	analytic_tradecraft	sat_evaluation_evidence	scholarly_peer_reviewed	2026-06-15	annual	Peer-reviewed article arguing for a more evidence-attentive structuring of SATs and stronger links to judgment and decision-science research.
[Whitesmith, 2019]	analytic_tradecraft	sat_evaluation_evidence	scholarly_peer_reviewed	2026-06-15	annual	Peer-reviewed ACH experiment used to keep confirmation-bias and serial-position claims specific to a study design rather than a general SAT guarantee.
[Mandel, 2020]	analytic_tradecraft	sat_evaluation_evidence	scholarly_peer_reviewed	2026-06-15	annual	Open Cambridge article testing whether ACH improves coherence of probabilistic judgments from uncertain evidence.
[Dhami, 2018]	analytic_tradecraft	forecasting_calibration_and_judgment	scholarly_peer_reviewed	2026-06-15	annual	Open Judgment and Decision Making article comparing ACH, coherentization, and aggregation for intelligence analysts' probability judgments.
[Tetlock, 2015b]	analytic_tradecraft	forecasting_calibration_and_judgment	scholarly_peer_reviewed	2026-06-15	annual	Peer-reviewed decision-science article connecting intelligence analysis improvement to forecasting, probability judgment, and uncertainty communication evidence.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Council, 2011]	analytic_tradecraft	analytic_cognition_and_bias	scholarly_public_report	2026-06-15	annual	National Academies report connecting behavioral and social science to intelligence-analysis training, judgment, and organizational improvement.
[on Intelligence, 2004]	analytic_tradecraft	intelligence_failure_postmortem	official_report	2026-06-15	biennial	Official Senate report on prewar Iraq intelligence assessments used as postmortem context for assumptions, dissent, caveats, and source-confidence failures.
[Activity, 2010]	analytic_tradecraft	forecasting_calibration_and_aggregation	official_primary	2026-06-15	annual	Official IARPA ACE program page on eliciting, weighting, and combining probabilistic judgments to improve intelligence forecasts.
[Activity, 2023]	analytic_tradecraft	agentic_analytic_assistance	official_primary	2026-06-15	annual	Official IARPA REASON program page on analyst-in-the-loop evidence and reasoning support for draft analytic reports.
[Helmer, 1963]	analytic_tradecraft	forecasting_calibration_and_aggregation	scholarly_peer_reviewed	2026-06-15	annual	Classic peer-reviewed Delphi-method article used as historical method context for structured expert elicitation and iterative judgment aggregation.
[Klein, 2007]	analytic_tradecraft	analytic_method_pedagogy	professional_practice	2026-06-15	annual	Professional practice article introducing the premortem as a structured way to surface possible failure causes before commitment.
[Marrin, 2012]	analytic_tradecraft	analytic_method_pedagogy	scholarly_book_metadata	2026-06-15	annual	Routledge scholarly book on linking intelligence-analysis scholarship and practice, used for tradecraft pedagogy and evidence-uptake framing.
[Svenmarck, 2021]	analytic_tradecraft	analytic_method_pedagogy	official_research_report	2026-06-15	annual	Swedish Defence Research Agency report summary on 42 structured analytic techniques for assessment and judgement of major events.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Service, 2021]	analytic_tradecraft	analytic_method_pedagogy	public_practice_guidance	2026-06-15	annual	JIPS technical brief on joint structured analysis techniques for collaborative humanitarian and development data analysis.
[Denzler, 2024]	analytic_tradecraft	analytic_cognition_and_bias	scholarly_peer_review	2026-06-15	annual	Peer-reviewed article revisiting psychological assumptions behind SATs and their relationship to analytic cognition.
[Mandel, 2024]	analytic_tradecraft	sat_evaluation_evidence	scholarly_peer_review	2026-06-15	annual	Peer-reviewed critical review of ACH used to frame ACH as a diagnostic and review aid with contested efficacy claims.
[Miksa, 2024]	analytic_tradecraft	analytic_method_pedagogy	scholarly_peer_review	2026-06-15	annual	Peer-reviewed article proposing assessment tabling as an integrated SAT and reasoning-visualization approach.
[Coulthart, 2025]	analytic_tradecraft	sat_evaluation_evidence	scholarly_peer_review	2026-06-15	annual	Peer-reviewed survey of SAT perspectives and use in an intelligence fusion-centre context, useful for adoption and training caveats.
[Gustafson, 2025]	analytic_tradecraft	analytic_method_pedagogy	scholarly_peer_review	2026-06-15	annual	Peer-reviewed article on cross-national SAT teaching used for pedagogy, transfer, and local-context caveats.
[McCarthy, 2024]	analytic_tradecraft	warning_intelligence	scholarly_peer_review_open	2026-06-15	annual	National Security Journal article evaluating Alternative Futures Analysis as an imaginative-thinking SAT and emphasizing purpose-fit and facilitator context.
[Ritchey, 2013]	analytic_tradecraft	analytic_method_pedagogy	scholarly_method_note	2026-06-15	annual	Swedish Morphological Society page explaining general morphological analysis as a method for structuring non-quantified complex problem spaces.
[Pherson, 2014b]	analytic_tradecraft	analytic_method_pedagogy	scholarly_textbook	2026-06-15	annual	SAGE/CQ Press textbook page for SAT case pedagogy and classroom exercises for analyst training.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Pherson, 2020]	analytic_tradecraft	analytic_method_pedagogy	scholarly_textbook	2026-06-15	annual	SAGE/CQ Press textbook page for critical-thinking questions, analytic techniques, uncertainty, graphics, and source evaluation in intelligence education.
[of the Army., 2006]	collection_management	humint_doctrine	official_primary	2026-06-16	annual	Verified official primary source for humint_doctrine; routed to HUMINT collection discipline; source operations; interrogation ethics and doctrine. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[of the Director of National Intelligence., 2008]	collection_management	humint_doctrine	official_primary	2026-06-16	annual	Verified official primary source for humint_doctrine; routed to HUMINT governance; IC collection management; CI integration. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[of the Director of National Intelligence., 2016]	collection_management	humint_doctrine	official_primary	2026-06-16	annual	Verified official primary source for humint_doctrine; routed to HUMINT deconfliction; CI integration; overseas collection coordination. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[to Study Governmental Operations with Respect to Intelligence Activities, Church Committeea]	historical_declassified_sources	humint_oversight_history	public_domain_primary	2026-06-16	annual	Verified public domain primary source for humint_oversight_history; routed to HUMINT history and oversight; IC accountability; CI doctrine history. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[to Study Governmental Operations with Respect to Intelligence Activities, Church Committeeb]	legal_oversight	sigint_oversight_history	public_domain_primary	2026-06-16	annual	Verified public domain primary source for sigint_oversight_history; routed to SIGINT oversight history; NSA authorities and limitations; domestic surveillance doctrine. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[of the Director of National Intelligence., 2007]	collection_management	humint_doctrine	official_primary	2026-06-16	annual	Verified official primary source for humint_doctrine; routed to HUMINT collection; document and media analyzeation; all-source integration. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[of the Joint Chiefs of Staff., 2012]	collection_management	collection_management_doctrine	official_primary	2026-06-16	annual	Verified official primary source for collection_management_doctrine; routed to All-source collection management; HUMINT/SIGINT/GEOINT integration; joint intelligence support. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Agency., n.d.]	collection_management	sigint_emanations_intelligence	official_primary	2026-06-16	annual	Verified official primary source for sigint_emanations_intelligence; routed to SIGINT fundamentals; emanations intelligence; EMSEC/TEMPEST history. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[National Security Agency, Various years]	historical_declassified_sigint_history	sigint_history	official_primary	2026-06-16	annual	Verified official primary source for sigint_history; routed to SIGINT history; NSA organizational development; cryptologic heritage; ELINT/TELINT history. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[of Standards and Technology., 2024a]	agentic_ai_security	cryptography_standards	official_primary	2026-06-16	semiannual	Verified official primary source for cryptography_standards; routed to Cryptography standards; post-quantum SIGINT resilience; communications security modernization. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[of Standards and Technology., 2024b]	agentic_ai_security	cryptography_standards	official_primary	2026-06-16	semiannual	Verified official primary source for cryptography_standards; routed to Cryptography standards; post-quantum digital signatures; authentication in collection systems. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[of Standards and Technology., 2024c]	agentic_ai_security	cryptography_standards	official_primary	2026-06-16	semiannual	Verified official primary source for cryptography_standards; routed to Cryptography standards; post-quantum signature diversity; long-term data integrity. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Office of the Director of National Intelligence, 2022]	osint_geoint	osint_doctrine	official_primary	2026-06-16	annual	Verified official primary source for osint_doctrine; routed to OSINT/PAI doctrine; commercially available information; privacy and civil liberties in collection. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[of the Joint Chiefs of Staff., 2017]	osint_geoint	geoint_doctrine	official_primary	2026-06-16	annual	Verified official primary source for geoint_doctrine; routed to GEOINT doctrine; imagery intelligence in joint operations; NGA role; GEOINT organizations. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Clark, 2020]	osint_geoint	geoint_tradecraft	scholarly_book_metadata	2026-06-16	annual	Verified scholarly book metadata source for geoint_tradecraft; routed to GEOINT history and doctrine; remote sensing intelligence; IMINT tradecraft. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Van Puyvelde, 2025]	osint_geoint	osint_methodology	scholarly_repository_record	2026-06-16	annual	Verified scholarly repository record source for osint_methodology; routed to OSINT definition and discipline; OSINT methodology; validation and verification; civil society OSINT. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[of the Director of National Intelligence., Current]	osint_geoint	osint_doctrine	official_primary	2026-06-16	annual	Verified official primary source for osint_doctrine; routed to OSINT sourcing standards; analytic product integrity; IC information sourcing discipline. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Agency., 2018]	osint_geoint	geoint_doctrine	official_primary	2026-06-16	annual	Verified official primary source for geoint_doctrine; routed to GEOINT doctrine; NGA mission; GEOINT principles and definitions. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[of the Director of National Intelligence., 2024]	osint_geoint	osint_doctrine	official_primary	2026-06-16	annual	Verified official primary source for osint_doctrine; routed to OSINT/PAI governance; CAI policy framework; privacy in collection. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Hutchins, 2011]	cyber_threat_intelligence	cyber_threat_intelligence	professional_documentation	2026-06-16	semiannual	Verified professional documentation source for cyber_threat_intelligence; routed to Cyber Intelligence Fundamentals; APT Threat Intelligence; Structured Analytic Techniques for Cyber. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Caltagirone, 2013]	cyber_threat_intelligence	cyber_threat_intelligence	professional_documentation	2026-06-16	semiannual	Verified professional documentation source for cyber_threat_intelligence; routed to Cyber Intelligence Fundamentals; APT Analysis; Structured Analytic Techniques for Cyber CTI. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[CISA, 2024]	cyber_threat_intelligence	apt_threat_intelligence	official_primary	2026-06-16	semiannual	Verified official primary source for apt_threat_intelligence; routed to Advanced Persistent Threats; ICS/OT Threat Intelligence; Supply Chain and Critical Infrastructure. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[NSA, 2023]	cyber_threat_intelligence	apt_threat_intelligence	official_primary	2026-06-16	semiannual	Verified official primary source for apt_threat_intelligence; routed to Advanced Persistent Threats; Cyber Intelligence Fundamentals; ICS/OT Security. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[DOE, 2022]	cyber_threat_intelligence	apt_threat_intelligence	official_primary	2026-06-16	semiannual	Verified official primary source for apt_threat_intelligence; routed to Advanced Persistent Threats; ICS/OT Security; MITRE ATT&CK for ICS. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[CISA., 2020]	cyber_threat_intelligence	supply_chain_intelligence_attacks	official_primary	2026-06-16	semiannual	Verified official primary source for supply_chain_intelligence_attacks; routed to Supply Chain Intelligence Attacks; Advanced Persistent Threats; Threat Intelligence Sharing. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Lee, 2016]	ics_ot_defense	historical_ics_incidents	official_primary	2026-06-16	semiannual	Verified official primary source for historical_ics_incidents; routed to Historical ICS Cyber Incidents; ICS/OT Security; Threat Intelligence Sharing for Critical Infrastructure. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[for Cybersecurity, ENISA]	cyber_threat_intelligence	cyber_threat_intelligence	official_primary	2026-06-16	semiannual	Verified official primary source for cyber_threat_intelligence; routed to Cyber Intelligence Fundamentals; Advanced Persistent Threats; ICS/OT Security; Threat Intelligence Sharing. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Boyens, 2022]	cyber_threat_intelligence	supply_chain_intelligence_attacks	official_primary	2026-06-16	semiannual	Verified official primary source for supply_chain_intelligence_attacks; routed to Supply Chain Intelligence Attacks; ICS/OT Security; Threat Intelligence Sharing. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Biden, 2021]	cyber_threat_intelligence	supply_chain_intelligence_attacks	official_primary	2026-06-16	semiannual	Verified official primary source for supply_chain_intelligence_attacks; routed to Supply Chain Intelligence Attacks; Cyber Intelligence Fundamentals; ICS/OT Security. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[of Incident Response and Teams, FIRST]	cyber_threat_intelligence	threat_intel_sharing_standards	official_primary	2026-06-16	semiannual	Verified official primary source for threat_intel_sharing_standards; routed to Threat Intelligence Sharing for Critical Infrastructure; Cyber Intelligence Fundamentals. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Corporation, NERC]	ics_ot_defense	ics_ot_security_standards	official_primary	2026-06-16	semiannual	Verified official primary source for ics_ot_security_standards; routed to ICS/OT Security; Critical Infrastructure Protection; Threat Intelligence Sharing for Critical Infrastructure. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Cherepanov, 2017]	ics_ot_defense	historical_ics_incidents	professional_documentation	2026-06-16	semiannual	Verified professional documentation source for historical_ics_incidents; routed to Historical ICS Cyber Incidents; ICS/OT Security; MITRE ATT&CK for ICS. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[ICS-CERT., 2010]	ics_ot_defense	historical_ics_incidents	official_primary	2026-06-16	semiannual	Verified official primary source for historical_ics_incidents; routed to Historical ICS Cyber Incidents; ICS/OT Security; MITRE ATT&CK for ICS. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[CISA., 2022]	ics_ot_defense	ics_ot_security_standards	official_primary	2026-06-16	semiannual	Verified official primary source for ics_ot_security_standards; routed to ICS/OT Security; Advanced Persistent Threats; MITRE ATT&CK for ICS. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[ICS., 2017]	ics_ot_defense	historical_ics_incidents	official_primary	2026-06-16	semiannual	Verified official primary source for historical_ics_incidents; routed to Historical ICS Cyber Incidents; ICS/OT Security; MITRE ATT&CK for ICS. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[for Network and Security, ENISA]	ics_ot_defense	ics_ot_security_standards	official_primary	2026-06-16	semiannual	Verified official primary source for ics_ot_security_standards; routed to ICS/OT Security; Critical Infrastructure Protection; MITRE ATT&CK for ICS context. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[of Staff., 2012]	cognitive_influence_security	information_operations_doctrine	official_primary	2026-06-16	annual	Verified official primary source for information_operations_doctrine; routed to Information Warfare and Cognitive Security; PSYOP and MISO Doctrine. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[of Staff., 2014b]	cognitive_influence_security	psyop_miso_doctrine	official_primary	2026-06-16	annual	Verified official primary source for psyop_miso_doctrine; routed to PSYOP and MISO Doctrine; Information Warfare and Cognitive Security. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Paul and Matthews., 2016]	cognitive_influence_security	active_measures_disinformation	professional_documentation	2026-06-16	annual	Verified professional documentation source for active_measures_disinformation; routed to Active Measures and Disinformation; Information Warfare and Cognitive Security. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Lazer, 2018]	cognitive_influence_security	disinformation_misinformation_science	scholarly_peer_reviewed	2026-06-16	annual	Verified scholarly peer reviewed source for disinformation_misinformation_science; routed to Active Measures and Disinformation; Information Warfare and Cognitive Security; Social Engineering. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Network, FinCEN]	financial_economic_security	finint_sar_reporting	official_primary	2026-06-16	annual	Verified official primary source for finint_sar_reporting; routed to Financial Intelligence (FININT). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[of Financial Intelligence Units., 2023]	financial_economic_security	finint_international_cooperation	official_primary	2026-06-16	annual	Verified official primary source for finint_international_coopera routed to Financial Intelligence (FININT). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[on Drugs and Crime, UNODC]	financial_economic_security	finint_aml_cft_international	official_primary	2026-06-16	annual	Verified official primary source for finint_aml_cft_internationa routed to Financial Intelligence (FININT). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Schott, 2006]	financial_economic_security	finint_aml_cft_international	official_primary	2026-06-16	annual	Verified official primary source for finint_aml_cft_internationa routed to Financial Intelligence (FININT). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Counterintelligence and Center, NCSCb]	counterintelligence_security	counterintelligence_strategy	official_primary	2026-06-16	annual	Verified official primary source for counterintelli- gence_strategy; routed to Counterintelligence (fundamentals + against non-state actors). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Counterintelligence and Center, NCSCa]	counterintelligence_source_integrity	counterintelligence_strategy	official_primary	2026-06-16	annual	Verified official primary source for counterintelligence_strategy; routed to Counterintelligence (fundamentals + against non-state actors). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Pennycook and Rand., 2021]	cognitive_influence_source_integrity	disinformation_cognitive_psychology	scholarly_repository	2026-06-16	annual	Verified scholarly repository record source for disinformation_cognitive_psychology; routed to Active Measures and Disinformation; Social Engineering; Information Warfare and Cognitive Security. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Starbird and Wilson., 2019]	cognitive_influence_source_integrity	active_measures_information_operations	scholarly_repository	2026-06-16	annual	Verified scholarly repository record source for active_measures_information_operations; routed to Active Measures and Disinformation; Information Warfare and Cognitive Security; Social Engineering. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Hoffman, 2007]	cognitive_influence_source_integrity	hybrid_warfare_doctrine	scholarly_repository	2026-06-16	annual	Verified scholarly repository record source for hybrid_warfare_doctrine; routed to Gray Zone / Hybrid Warfare / Non-State Actor Intelligence / Irregular Warfare. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Mazarr, 2015]	cognitive_influence_security	gray_zone_competition_doctrine	scholarly_book_metadata	2026-06-16	annual	Verified scholarly book metadata source for gray_zone_competition_doc routed to Gray Zone / Hybrid Warfare / Non-State Actor Intelligence / Irregular Warfare. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[of Defense., 2020]	cognitive_influence_security	irregular_warfare_strategy	official_primary	2026-06-16	annual	Verified official primary source for irregular_warfare_strategy; routed to Gray Zone / Hybrid Warfare / Non-State Actor Intelligence / Irregular Warfare. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[of Staff., 2014a]	collection_management	special_operations_doctrine	official_primary	2026-06-16	annual	Verified official primary source for special_operations_doctrine; routed to Gray Zone / Hybrid Warfare / Non-State Actor Intelligence / Irregular Warfare; Counterintelligence. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Cialdini, 1984]	cognitive_influence_security	social_engineering_influence	scholarly_psychology	2026-06-16	annual	Verified scholarly book metadata source for social_engineering_influence routed to Social Engineering; Active Measures and Disinformation; Information Warfare and Cognitive Security. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[of Excellence., 2021]	cognitive_influence_security	hybrid_warfare_stratcom	official_primary	2026-06-16	annual	Verified official primary source for hybrid_warfare_stratcom; routed to Gray Zone / Hybrid Warfare / Non-State Actor Intelligence / Irregular Warfare; Active Measures and Disinformation. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[of Staff., 2013]	osint_geoint	imint_joint_intelligence_do	official_primary	2026-06-16	annual	Verified official primary source for imint_joint_intelligence_do routed to Imagery Intelligence (IMINT); Counterintelligence. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Pamment and Smith., 2022]	cognitive_influence_security	active_measures_attribution	official_primary	2026-06-16	annual	Verified official primary source for active_measures_attribution; routed to Active Measures and Disinformation; Counterintelligence; Information Warfare and Cognitive Security. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Andrew, 1990]	historical_declassified	intelligence_history_soviet	scholarly_book_metadata	2026-06-16	annual	Verified scholarly book metadata source for intelligence_history_soviet; routed to Historical Intelligence Services (Soviet/Russian); KGB organizational doctrine and operations overview. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Andrew, 1999]	historical_declassified_intelligence	history_soviet	scholarly_book_metadata	2026-06-16	annual	Verified scholarly book metadata source for intelligence_history_soviet; routed to Historical Intelligence Services (Soviet/Russian); primary-source archival history of KGB. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Andrew, 2009]	historical_declassified_intelligence	history_british_allied	scholarly_book_metadata	2026-06-16	annual	Verified scholarly book metadata source for intelligence_history_british_allied; routed to Historical Intelligence Services (British/Allied); institutional history of domestic security intelligence. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Weiner, 2007]	historical_declassified_intelligence	history_american	scholarly_book_metadata	2026-06-16	annual	Verified scholarly book metadata source for intelligence_history_american; routed to Historical Intelligence Services (American); CIA institutional failures and analytic dysfunction. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[to Study Governmental Operations with Respect to Intelligence Activities., 1976]	legal_oversight	legal_oversight_intelligence	public_domain_primary	2026-06-16	annual	Verified public domain primary source for legal_oversight_intelligence; routed to Legal Authorities and Constraints; Historical Intelligence Services (American); oversight reform history. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Tversky, 1974]	analytic_tradecraft	cognitive_bias_foundations	scholarly_repository_record	2026-06-16	annual	Verified scholarly repository record source for cognitive_bias_foundations; routed to Cognitive Security (neurocognitive mechanisms); Epistemic Rigor & Analytic Tradecraft (cognitive bias in analysis). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Kahneman, 2011]	analytic_tradecraft	cognitive_bias_foundations	scholarly_book_metadata	2026-06-16	annual	Verified scholarly book metadata source for cognitive_bias_foundations; routed to Cognitive Security (dual-process neurocognitive mechanisms); Epistemic Rigor & Analytic Tradecraft. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Lewandowsky, 2021]	cognitive_influence_security	cognitive_security_inoculation	scholarly_peer_reviewed	2026-06-16	annual	Verified scholarly peer reviewed source for cognitive_security_inoculation; routed to Cognitive Security (psychological inoculation & prebunking); Cognitive Security Operations. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Lewandowsky, 2020]	cognitive_influence_security	cognitive_security_inoculation	scholarly_repository_record	2026-06-16	annual	Verified scholarly repository record source for cognitive_security_inoculation; routed to Cognitive Security (psychological inoculation & prebunking); corrections and debunking protocol. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Pennycook, 2021]	cognitive_influence_security	cognitive_security_misinformation	scholarly_peer_reviewed	2026-06-16	annual	Verified scholarly peer reviewed source for cognitive_security_misinformatio routed to Cognitive Security (psychological inoculation & prebunking); Cognitive Security Operations (scalable interventions). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Tetlock, 2005]	analytic_tradecraft	analytic_tradecraft_forecasting	scholarly_book_metadata	2026-06-16	annual	Verified scholarly book metadata source for analytic_tradecraft_forecasting routed to Epistemic Rigor & Analytic Tradecraft (Advanced Analysis Methods); forecasting accuracy and calibration. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Tetlock, 2015a]	analytic_tradecraft	analytic_tradecraft_forecasting	scholarly_book_metadata	2026-06-16	annual	Verified scholarly book metadata source for analytic_tradecraft_forecasting routed to Epistemic Rigor & Analytic Tradecraft (Advanced Analysis Methods); Good Judgment Project findings. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Congress., 1978]	legal_oversight	legal_authorities_surveillance	official_primary	2026-06-16	annual	Verified official primary source for legal_authorities_surveillance routed to Legal Authorities and Constraints; oversight of domestic electronic surveillance. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Congress., 2001]	legal_oversight	legal_authorities_surveillance	official_primary	2026-06-16	annual	Verified official primary source for legal_authorities_surveillance routed to Legal Authorities and Constraints; post-9/11 surveillance expansion. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Congress., 2015]	legal_oversight	legal_authorities_surveillance	official_primary	2026-06-16	annual	Verified official primary source for legal_authorities_surveillance routed to Legal Authorities and Constraints; surveillance reform and civil liberties. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Reagan, 1981]	legal_oversight	legal_authorities_intelligence_collection	official_primary	2026-06-16	annual	Verified official primary source for legal_authorities_intelligence_collection routed to Legal Authorities and Constraints; EO-based authorities for IC collection. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Quinlan, 2007]	legal_oversight	ethics_of_intelligence	scholarly_repository_record	2026-06-16	annual	Verified scholarly repository record source for ethics_of_intelligence; routed to Ethics of Intelligence and Cognitive Security; just-intelligence theory. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Omand, 2010]	legal_oversight	ethics_of_intelligence	scholarly_book_metadata	2026-06-16	annual	Verified scholarly book metadata source for ethics_of_intelligence; routed to Ethics of Intelligence and Cognitive Security; legal and ethical constraints on secret intelligence; oversight principles. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Omand, 2018]	legal_oversight	ethics_of_intelligence	scholarly_book_metadata	2026-06-16	annual	Verified scholarly book metadata source for ethics_of_intelligence; routed to Ethics of Intelligence and Cognitive Security; HUMINT ethics; surveillance ethics; oversight accountability. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Russell, 2020]	agentic_ai_governance	agent_foundations	scholarly_repository_record	2026-06-16	semiannual	Verified scholarly repository record source for agent_foundations; routed to Foundations of AGEINT (agent definition, PEAS framework, rational agents); AGEINT Python Code Library. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Rao, 1995]	agentic_ai_governance	agent_foundations	scholarly_repository_record	2026-06-16	semiannual	Verified scholarly repository record source for agent_foundations; routed to Foundations of AGEINT (agent architectures); Design Patterns & Archetypes (goal-directed agent archetypes). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Vaswani, 2017]	agentic_ai_governance	llm_architecture	scholarly_preprint	2026-06-16	semiannual	Verified scholarly preprint source for llm_architecture; routed to Foundations of AGEINT (LLM substrate); LangChain/LangGraph Patterns appendix; CrewAI appendix; AutoGen/MCP appendix. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Yao, 2023b]	agentic_ai_governance	agentic_reasoning	scholarly_preprint	2026-06-16	semiannual	Verified scholarly preprint source for agentic_reasoning; routed to Foundations of AGEINT (reasoning architectures); Design Patterns & Archetypes (planning patterns); LangChain/LangGraph Patterns appendix. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Lewis, 2020]	agentic_ai_governance	agentic_memory	scholarly_preprint	2026-06-16	semiannual	Verified scholarly preprint source for agentic_memory; routed to Foundations of AGEINT (agent memory); Design Patterns & Archetypes (RAG architecture); LangChain/LangGraph Patterns appendix; AGEINT Python Code Li…. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Patil, 2023]	agentic_ai_governance	tool_use_agents	scholarly_preprint	2026-06-16	semiannual	Verified scholarly preprint source for tool_use_agents; routed to Foundations of AGEINT (tool-use patterns); AGEINT Python Code Library; LangChain/LangGraph Patterns appendix. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Qin, 2023]	agentic_ai_governance	tool_use_agents	scholarly_preprint	2026-06-16	semiannual	Verified scholarly preprint source for tool_use_agents; routed to Foundations of AGEINT (tool-use); AGEINT Python Code Library; LangChain/LangGraph Patterns appendix. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Wu, 2023]	agentic_ai_governance	multi_agent_frameworks	scholarly_preprint	2026-06-16	semiannual	Verified scholarly preprint source for multi_agent_frameworks; routed to AutoGen and MCP Patterns appendix; Frameworks & Infrastructure; CrewAI appendix (comparison context). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[LangChain, 2025a]	agentic_ai_governance	agentic_framework_docs	professional_documentation	2026-06-16	semiannual	Verified professional documentation source for agentic_framework_docs; routed to LangChain/LangGraph Patterns appendix; AGEINT Python Code Library. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[LangChain, 2025b]	agentic_ai_governance	agentic_framework_docs	professional_documentation	2026-06-16	semiannual	Verified professional documentation source for agentic_framework_docs; routed to LangChain/LangGraph Patterns appendix; AGEINT Python Code Library; Frameworks & Infrastructure. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[CrewAI, 2025]	agentic_ai_governance	agentic_framework_docs	professional_documentation	2026-06-16	semiannual	Verified professional documentation source for agentic_framework_docs; routed to CrewAI Multi-Agent appendix; Frameworks & Infrastructure. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Liang, 2022]	agentic_ai_governance	llm_evaluation	scholarly_preprint	2026-06-16	semiannual	Verified scholarly preprint source for llm_evaluation; routed to Frameworks & Infrastructure (model evaluation); Security & Adversarial Considerations (model capability assessment); AGEINT Python Code Library. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Srivastava, 2022]	agentic_ai_governance	llm_evaluation	scholarly_preprint	2026-06-16	semiannual	Verified scholarly preprint source for llm_evaluation; routed to Frameworks & Infrastructure (model evaluation); Security & Adversarial Considerations; AGEINT Python Code Library. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Perez, 2022]	agentic_ai_security	adversarial_ai_security	scholarly_preprint	2026-06-16	semiannual	Verified scholarly preprint source for adversarial_ai_security; routed to Security & Adversarial Considerations; ATT&CK & Kill Chain Templates appendix; Cognitive Security & Inoculation appendix. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Ericsson, 1993]	education_assessment	cognitive_performance	scholarly_repository_record	2026-06-16	annual	Verified scholarly repository record source for cognitive_performance; routed to Productivity Intelligence & Cognitive Performance (cognitive athlete, deliberate practice); Instructor Capstone/Rubric/Red-Team Pack appendix. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[Cepeda, 2006]	education_assessment	cognitive_performance	scholarly_repository_record	2026-06-16	annual	Verified scholarly repository record source for cognitive_performance; routed to Productivity Intelligence & Cognitive Performance (information architecture, spaced repetition); Instructor Capstone/Rubric/Red-Team Pack appendix. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Walker, 2006]	education_assessment	cognitive_performance	scholarly_repository_record	2026-06-16	annual	Verified scholarly repository record source for cognitive_performance; routed to Productivity Intelligence & Cognitive Performance (sleep and cognition); Cognitive Security & Inoculation appendix. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Kaplan, 1989]	education_assessment	cognitive_performance	scholarly_book_metadata	2026-06-16	annual	Verified scholarly book metadata source for cognitive_performance; routed to Productivity Intelligence & Cognitive Performance (attention restoration, information architecture); Cognitive Security & Inoculation appendix. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Anchor	Domain	Lane	Tier	Checked	Refresh	Curriculum use
[of Standards and Technology., 2024]	agentic_ai_security	cryptographic_standards	official_draft	2026-06-16	semiannual	Verified official draft source for cryptographic_standards; routed to Cryptographic Methods appendix; Security & Adversarial Considerations. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Weng, 2023]	agentic_ai_governance	agentic_design_principles	professional_documentation	2026-06-16	semiannual	Verified professional documentation source for agentic_design_principles; routed to Foundations of AGEINT (agent memory, tool use, planning); Design Patterns & Archetypes. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

2.12 Source lane map: provenance lanes, support strength, and refresh context

Source lane	Anchor count	Refresh cadence	Claim scope
accessibility_digital_inclusion	4	annual, quarterly, semiannual	4 scoped claim families
active_measures_attribution	1	annual	Supports bounded AGEINT discussion of active_measures_attribution and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
active_measures_disinformation	1	annual	Supports bounded AGEINT discussion of active_measures_disinformation and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
active_measures_information_operations	1	annual	Supports bounded AGEINT discussion of active_measures_information_operations and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
adversarial_ai_security	1	semiannual	Supports bounded AGEINT discussion of adversarial_ai_security and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
agent_foundations	2	semiannual	Supports bounded AGEINT discussion of agent_foundations and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
agent_incident_response	7	annual, quarterly, semiannual	7 scoped claim families
agent_interoperability_standards	12	annual, quarterly, semiannual	12 scoped claim families
agentic_ai_governance	21	annual	8 scoped claim families
agentic_ai_security	2	annual, semiannual	2 scoped claim families
agentic_ai_security_governance	1	quarterly	agentic AI adoption and security-governance context, not an AGEINT benchmark
agentic_analytic_assistance	1	annual	Supports bounded claims that AI-enabled reasoning systems can assist evidence discovery and reasoning review while retaining analyst responsibility.
agentic_design_principles	1	semiannual	Supports bounded AGEINT discussion of agentic_design_principles and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.

Source lane	Anchor count	Refresh cadence	Claim scope
agentic_framework_docs	3	semiannual	Supports bounded AGEINT discussion of agentic_framework_docs and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
agentic_memory	1	semiannual	Supports bounded AGEINT discussion of agentic_memory and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
agentic_reasoning	1	semiannual	Supports bounded AGEINT discussion of agentic_reasoning and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
ai_conformity_compliance	7	annual, quarterly, semiannual	7 scoped claim families
ai_enabled_analysis_boundary	9	annual, semiannual	9 scoped claim families
ai_ethics_data_governance	10	annual	curriculum grounding and source-backed synthesis
ai_red_team_assurance	14	annual, quarterly, semiannual	14 scoped claim families
algorithmic_transparency_reporting	2	quarterly	2 scoped claim families
analytic_cognition_and_bias	6	annual	6 scoped claim families
analytic_epistemology	1	annual	epistemic-framing support for calibrated claims and reviewer challengeability
analytic_method_design	3	annual	3 scoped claim families
analytic_method_pedagogy	9	annual	9 scoped claim families
analytic_outreach_governance	1	annual	analytic-outreach governance support for expert engagement and risk controls
analytic_product_dissemination	1	annual	analytic-product utility, discoverability, and dissemination-governance support
analytic_production_workflow	1	annual	workflow and analytic-production support for iterative, reviewable tradecraft artifacts
analytic_tradecraft	7	annual	2 scoped claim families
analytic_tradecraft_evidence	5	annual	5 scoped claim families
analytic_tradecraft_forecasting	2	annual	Supports bounded AGEINT discussion of analytic_tradecraft_forecasting and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
analytic_uncertainty_language	4	annual	4 scoped claim families
apt_threat_intelligence	3	semiannual	Supports bounded AGEINT discussion of apt_threat_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
assurance_evaluation_evidence	8	annual, quarterly, semiannual	8 scoped claim families
classification_marking_governance	1	annual	classification-marking context for caveat and dissemination-boundary lessons
cognitive_active_inference	9	annual	9 scoped claim families

Source lane	Anchor count	Refresh cadence	Claim scope
cognitive_bias_foundations	2	annual	Supports bounded AGEINT discussion of cognitive_bias_foundations and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
cognitive_influence_security	13	annual	10 scoped claim families
cognitive_performance	4	annual	Supports bounded AGEINT discussion of cognitive_performance and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
cognitive_resilience_evidence	1	annual	Peer-reviewed Science Advances study testing psychological inoculation videos for improving misinformation resilience at scale, with bounded transfer from measured outcomes to curriculum claims
cognitive_security_inoculation	2	annual	Supports bounded AGEINT discussion of cognitive_security_inoculation and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
cognitive_security_misinformation	1	annual	Supports bounded AGEINT discussion of cognitive_security_misinformation and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
collection_management	2	annual	curriculum grounding and source-backed synthesis
collection_management_doctrine	1	annual	Supports bounded AGEINT discussion of collection_management_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
counterintelligence_program_governance	2	annual, quarterly	2 scoped claim families
counterintelligence_source_integrity	7	annual	6 scoped claim families
counterintelligence_strategy	2	annual	Supports bounded AGEINT discussion of counterintelligence_strategy and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
cross_border_data_spaces	4	semiannual	4 scoped claim families

Source lane	Anchor count	Refresh cadence	Claim scope
cryptographic_standards	1	semiannual	Supports bounded AGEINT discussion of cryptographic_standards and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
cryptography_standards	3	semiannual	Supports bounded AGEINT discussion of cryptography_standards and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
current_threat_baseline	1	annual	public threat-context grounding and warning-topic baseline, not operational targeting or AGEINT benchmark evidence
cyber_defense_guidance_index	1	quarterly	defensive cyber guidance index support for source routing and refresh duties
cyber_threat_intelligence	17	annual, semiannual	8 scoped claim families
dataset_documentation	2	annual	2 scoped claim families
declassified_analytic_history	2	annual	2 scoped claim families
declassified_reconnaissance_history	1	annual	declassified reconnaissance history support for historical and GEOINT source-provenance lessons
defense_osint_governance	1	annual	public OSINT governance and professionalization support, not collection procedure or live targeting guidance
disinformation_cognitive_psychology	1	annual	Supports bounded AGEINT discussion of disinformation_cognitive_psychology and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
disinformation_misinformation_science	1	annual	Supports bounded AGEINT discussion of disinformation_misinformation_science and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
economic_security_review	1	annual	economic-security and due-diligence governance support for threat-analysis framing
education_assessment	6	annual, semiannual	6 scoped claim families
ethics_of_intelligence	3	annual	Supports bounded AGEINT discussion of ethics_of_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
financial_economic_security	8	annual	curriculum grounding and source-backed synthesis

Source lane	Anchor count	Refresh cadence	Claim scope
finint_aml_cft_international	2	annual	Supports bounded AGEINT discussion of finint_aml_cft_international and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
finint_international_cooperation	1	annual	Supports bounded AGEINT discussion of finint_international_cooperation and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
finint_sar_reporting	1	annual	Supports bounded AGEINT discussion of finint_sar_reporting and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
forecasting_calibration_evidence	6	annual	6 scoped claim families
foreign_disclosure_governance	1	annual	foreign-disclosure governance support for release-boundary and control-marking lessons
geoint_data_governance	1	annual	GEOINT data-governance and digital-transformation context for modular source substrate claims
geoint_doctrine	2	annual	Supports bounded AGEINT discussion of geoint_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
geoint_professional_doctrine	1	annual	GEOINT doctrine and geospatial-intelligence framing support
geoint_tradecraft	1	annual	Supports bounded AGEINT discussion of geoint_tradecraft and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
governed_intelligence_cycle	2	annual	curriculum grounding and source-backed synthesis
gray_zone_competition_doctrine	1	annual	Supports bounded AGEINT discussion of gray_zone_competition_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
historical_declassified_sources	4	annual	curriculum grounding and source-backed synthesis

Source lane	Anchor count	Refresh cadence	Claim scope
historical_ics_incidents	4	semiannual	Supports bounded AGEINT discussion of historical_ics_incidents and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
human_rights_governance	6	annual, semiannual	6 scoped claim families
humint_doctrine	4	annual	Supports bounded AGEINT discussion of humint_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
humint_oversight_history	1	annual	Supports bounded AGEINT discussion of humint_oversight_history and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
hybrid_warfare_doctrine	1	annual	Supports bounded AGEINT discussion of hybrid_warfare_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
hybrid_warfare_stratcom	1	annual	Supports bounded AGEINT discussion of hybrid_warfare_stratcom and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
ic_information_environment_risk	2	annual	2 scoped claim families
ic_public_transparency	7	quarterly	7 scoped claim families
ics_ot_defense	10	annual	curriculum grounding and source-backed synthesis
ics_ot_security_standards	3	semiannual	Supports bounded AGEINT discussion of ics_ot_security_standards and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
imint_joint_intelligence_doctrine	1	annual	Supports bounded AGEINT discussion of imint_joint_intelligence_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.

Source lane	Anchor count	Refresh cadence	Claim scope
information_operations_doctrine	1	annual	Supports bounded AGEINT discussion of information_operations_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
integrated_mission_management	1	annual	mission-management governance support for requirements-to-evidence substrate design
intelligence_diplomacy_governance	1	annual	governance context for intelligence diplomacy and partner-engagement boundaries
intelligence_failure_postmortem	9	annual, biennial	9 scoped claim families
intelligence_history_american	1	annual	Supports bounded AGEINT discussion of intelligence_history_american and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
intelligence_history_british_allied	1	annual	Supports bounded AGEINT discussion of intelligence_history_british_allied and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
intelligence_history_soviet	2	annual	Supports bounded AGEINT discussion of intelligence_history_soviet and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
intelligence_profession_literature	4	annual	4 scoped claim families
intelligence_writing_and_review	3	annual	3 scoped claim families
irregular_warfare_strategy	1	annual	Supports bounded AGEINT discussion of irregular_warfare_strategy and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
learner_support_accommodations	1	semiannual	learner support plans, accessibility exception documentation, alternative means, and artifact remediation
legal_authorities_intelligence_collection	1	annual	Supports bounded AGEINT discussion of legal_authorities_intelligence_collection and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.

Source lane	Anchor count	Refresh cadence	Claim scope
legal_authorities_surveillance	3	annual	Supports bounded AGEINT discussion of legal_authorities_surveillance and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
legal_oversight	9	annual	curriculum grounding and source-backed synthesis
legal_oversight_intelligence	1	annual	Supports bounded AGEINT discussion of legal_oversight_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
llm_architecture	1	semiannual	Supports bounded AGEINT discussion of llm_architecture and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
llm_evaluation	2	semiannual	Supports bounded AGEINT discussion of llm_evaluation and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
model_card_reporting	1	annual	model documentation cards, intended-use statements, evaluation caveats, and release notes
model_data_provenance	14	annual, quarterly, semiannual	14 scoped claim families
multi_agent_frameworks	1	semiannual	Supports bounded AGEINT discussion of multi_agent_frameworks and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
national_intelligence_governance	1	annual	IC governance and national-intelligence production context
non_state_engagement_governance	1	annual	non-state engagement governance support for source, outreach, and no-tasking boundaries
opsec_doctrine_governance	1	biennial	Provides official historical OPSEC policy context for critical-information protection and public doctrine framing; not an operational OPSEC playbook.
osint_doctrine	3	annual	Supports bounded AGEINT discussion of osint_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
osint_geoint	6	annual	2 scoped claim families

Source lane	Anchor count	Refresh cadence	Claim scope
osint_methodology	1	annual	Supports bounded AGEINT discussion of osint_methodology and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
privacy_ip_governance	3	annual	curriculum grounding and source-backed synthesis
procurement_performance_monitoring	1	quarterly	AI procurement monitoring, vendor demonstrations, acquisition criteria, QASP evidence, and performance review
procurement_vendor_governance	4	annual, quarterly, semiannual	4 scoped claim families
psyop_miso_doctrine	1	annual	Supports bounded AGEINT discussion of psyop_miso_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
public_sector_agentic_ai	5	quarterly, semiannual	5 scoped claim families
public_sector_transparency	3	annual, quarterly, semiannual	3 scoped claim families
records_retention_auditability	5	annual, quarterly, semiannual	5 scoped claim families
rights_impact_privacy	4	annual, quarterly, semiannual	4 scoped claim families
risk_exception_governance	1	quarterly	risk exception governance, AI maturity plans, data traceability, public trust, and oversight capacity
sat_evaluation_evidence	13	annual	13 scoped claim families
secure_release_change_control	9	annual, quarterly, semiannual	9 scoped claim families
sigint_emanations_intelligence	1	annual	Supports bounded AGEINT discussion of sigint_emanations_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
sigint_history	1	annual	Supports bounded AGEINT discussion of sigint_history and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
sigint_oversight_history	1	annual	Supports bounded AGEINT discussion of sigint_oversight_history and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
social_engineering_influence_psychology	1	annual	Supports bounded AGEINT discussion of social_engineering_influence_psychology and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.

Source lane	Anchor count	Refresh cadence	Claim scope
source_construction_reporting	1	annual	PRISMA-S reporting guideline for documenting literature searches, search strategies, information sources, limits, records, and reproducibility details
special_operations_doctrine	1	annual	Supports bounded AGEINT discussion of special_operations_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
supply_chain_intelligence_attacks	3	semiannual	Supports bounded AGEINT discussion of supply_chain_intelligence_attacks and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
supply_chain_risk_governance	1	annual	supply-chain risk governance support for defensive procurement and assurance lessons
synthetic_media_provenance	4	annual, semiannual	4 scoped claim families
tearlines_and_release_governance	1	annual	tearline and release-governance support for public-facing evidence boundaries
threat_intel_sharing_standards	1	semiannual	Supports bounded AGEINT discussion of threat_intel_sharing_standards and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
tool_use_agents	2	semiannual	Supports bounded AGEINT discussion of tool_use_agents and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
warning_intelligence	3	annual	3 scoped claim families
workforce_governance	5	annual, quarterly, semiannual	5 scoped claim families

2.13 Safe substitution matrix: defensive artifacts for risky inherited motifs

Source motif	Unsafe source motif	Safe curriculum substitute	Blocked context
AGEINT patterns	raw source motifs can imply autonomous tasking, monitoring, response, or deception	identity-preserving pattern registry plus tabletop, audit, provenance, and governance exercises	deployment, live target tasking, or external action
OSINT tools	broad scraping, exposed-service lookup, credentialed search, or identity exposure	tool-governance audit over instructor-provided records, toy inputs, and source-quality cards	live collection expansion or private-data discovery
GEOINT	facility assessment, force assessment, geolocation targeting, or pattern-of-life inference	provided imagery metadata quality audit with synthetic change examples and uncertainty notes	live facility assessment or tracking
SOC and CTI	autonomous response, exploitability claims, indicator publishing, or production-system action	fabricated-alert tabletop triage with ATT&CK mapping, severity rationale, and debrief evidence	production containment, exploitation, scanning, or blocking
HUMINT and CI	persona construction, contact handling, elicitation, deception, or source exposure	synthetic identity-and-provenance ethics audit with role-play records and review rubrics	impersonation, covert contact, or operational-security support
Cognitive influence	covert persuasion, microtargeting, audience manipulation, or intervention delivery	opt-in media-literacy lesson plan using synthetic materials and transparent prebunking labels	campaign design or audience-targeted persuasion
ICS and OT	facility monitoring, control action, safety-system interference, or cyber-physical response	owned-lab or synthetic process-safety tabletop with logs, rollback, and human approval gates	real plant operations, live devices, or unsafe control changes

2.14 Capstone workflow: phase sequence, artifacts, and reviewer gates

Phase	Artifact	Review gate
Question	accountable learning question and excluded-action list	instructor confirms scope, allowed data, and rights impact
Source canon	source-lane map with guide citations, verified anchors, and refresh dates	citation keys resolve and source identity lock remains stable
Evidence ledger	claim, evidence, uncertainty, confidence, and reviewer register	every material claim has a source, caveat, and owner
Safe lab	synthetic or public dataset packet, tool allowlist, and stop conditions	no live target, private data, external action, or unsafe cyber-physical step
Assurance	evaluation rubric, failure-mode drill, rights map, and remediation note	human reviewer signs off before presentation or reuse
Debrief	capstone memo with lessons, residual risk, refresh triggers, and handoff owner	all unresolved questions and future approvals are explicit

2.15 Capstone model-answer exemplars: strong evidence packets and revision triggers

These exemplars show the expected shape of a strong answer without prescribing a single conclusion. Use them as answer-key patterns for selected capstone reviews.

Capstone pattern	Model-answer evidence	What earns revision
Source-quality packet	Names the `ageintNNN` source key, source lane, direct evidence, caveat, uncertainty, and refresh trigger.	Claim cites a summary, omits the source key, or hides uncertainty.
Safe-lab packet	States the learning question, allowed inputs, excluded actions, tool allowlist, stop condition, and reviewer gate.	Uses private data, live targets, credentialed access, or an unreviewed tool path.
Assurance packet	Connects rubric score, rights impact, accessibility check, remediation owner, and debrief handoff.	Treats the score as proof, omits affected users, or leaves no owner for retest.

2.16 Accessibility and UDL review: learner access, modality checks, and accommodation evidence

Step	Artifact	Review question
Access baseline	WCAG/UDL needs note	Can every learner perceive, operate, understand, and complete the artifact without a hidden access barrier?
Learner variability	multiple-means design note	Are engagement, representation, and action or expression options available before remediation is requested?
Assistive technology	screen-reader, keyboard, contrast, caption, and plain-language check	Can the artifact be reviewed with common assistive workflows and documented alternatives?
Public-service duty	Title II or institutional-accessibility obligation note	If a public or institutional audience uses this artifact, are contractor and service-access duties visible?
Remediation evidence	defect log, owner, due date, and retest result	Are accessibility defects tracked to closure before the artifact is reused?

2.17 Procurement and vendor oversight: tool governance, revocation, and vendor evidence

Step	Artifact	Review question
Need and authority	procurement rationale and legal authority card	Is the vendor capability tied to a valid learning, governance, or defensive need?
Market and vendor transparency	vendor disclosure, subcontractor, data-use, and conflict-of-interest register	Can reviewers see who provides the tool, what data it touches, and which dependencies matter?
Evaluation criteria	weighted criteria for accessibility, privacy, security, provenance, and reversibility	Are evaluation criteria explicit before tool selection rather than rationalized afterward?
Contract controls	logging, deletion, audit, incident, accessibility, and termination clauses	Can the institution pause, audit, remediate, or exit the vendor relationship?
Lifecycle monitoring	renewal evidence, performance review, incident record, and refresh trigger	Does oversight continue after award and before classroom reuse?

2.18 HRIA and DPIA worksheet: rights impact, privacy review, and residual risk

Dimension	Prompt	Evidence
Purpose and authority	What public, educational, or defensive purpose justifies the processing or analysis?	scope card, excluded-action list, and decision owner
Data subjects and affected groups	Who could be affected directly, indirectly, or through downstream reuse?	stakeholder map, vulnerability note, and accessibility considerations
High-risk processing trigger	Does the activity involve sensitive data, profiling, automated evaluation, large-scale processing, or systematic monitoring?	DPIA trigger checklist and mitigation owner
Rights and safeguards	How are privacy, equality, expression, access, contestability, and redress protected?	rights-impact note, safeguard register, and escalation path
Residual risk and refresh	What remains uncertain, who accepts it, and what source or incident would reopen review?	residual-risk decision, review date, and source-refresh trigger

2.19 Data lineage registry: source identity, transformations, retention, and review

Object	Lineage field	Quality gate
Source citation	`ageintNNN`, title, URL, checked date, and source identity status	citation key resolves and reference identity is locked or append-only
Verified anchor	lane, tier, verification method, claim scope, stakeholder role, and assurance use	direct official, standards, public-domain, or scholarly URL was reviewed
Dataset or scenario	origin, license, sensitivity class, transformations, and retention rule	public, synthetic, owned-lab, or instructor-provided data only
Agent transcript	prompt, model context, tool allowlist, budget, reviewer, and blocked actions	no external action, live target, private data, or unsafe cyber-physical step
Final artifact	claim ledger, uncertainty note, accessibility status, rights review, and refresh owner	another reviewer can reproduce and challenge the artifact

2.20 Assessment integrity protocol: declared agent use, grading evidence, and human judgment

Control	Student evidence	Instructor check
Accountable AI use	tool-use declaration and prompt/output appendix	AI assistance is allowed, visible, bounded, and aligned with the assignment
Independent reasoning	assumptions, alternatives, uncertainty, and confidence statement	student judgment is separable from agent-generated drafting
Citation integrity	source spine, verified anchors, and claim ledger	claims are not source-laundered through agent prose
Synthetic lab boundary	allowed-inputs card, excluded actions, and stop conditions	activity remains public, benign, owned-lab, synthetic, defensive, and reversible
Feedback and revision	rubric self-score, reviewer notes, and remediation log	revision evidence addresses the actual deficiency before reuse

2.21 Agent incident response drill: pause, revoke, preserve, recover, and debrief

Phase	Drill action	Artifact
Prepare	define agent scope, tool permissions, logs, escalation roles, and stop conditions	incident play card and contact matrix
Detect	identify anomalous output, policy drift, source-laundering, data exposure, or unsafe tool request	synthetic incident ticket and evidence snapshot
Contain	pause the workflow, revoke tool access, preserve records, and route to human review	containment decision and access-change log
Recover	restore a known-safe prompt, dataset, tool profile, or rubric state	rollback note and retest result
Debrief	record root cause, learner impact, rights impact, vendor implication, and refresh trigger	post-incident memo and owner assignment

2.22 Role-based competency map: responsibilities, evidence owners, and assurance roles

Role	Competency	Evidence
Learner analyst	separate claim, evidence, uncertainty, confidence, and source quality	claim ledger and reflective memo
Instructor	facilitate safe labs, assess integrity, and preserve accessibility	rubric, UDL review, and debrief notes
Source steward	lock source identities, verify new anchors, and maintain refresh triggers	Section 2.12 and Section 80.3
Assurance reviewer	test failure modes, adversarial assumptions, tool boundaries, and incident response	red-team review, incident drill, and remediation record
Rights and procurement reviewer	evaluate privacy, accessibility, vendor, public transparency, and human-rights impacts	HRIA/DPIA worksheet and procurement oversight packet

2.23 Adversarial assurance cycle: challenge rows, remediation owners, and retest evidence

Stage	Challenge question	Artifact
Misuse case	How could the module be misread as operational, unfair, inaccessible, or overconfident?	misuse-case card and safe-substitution decision
Control challenge	Which authority, data, tool, rights, or review control would fail first?	control challenge matrix
Evidence attack	Can a claim survive source verification, provenance review, and counter-evidence?	challenged claim ledger
Incident rehearsal	What happens if an agent drifts, leaks context, fabricates support, or requests unsafe action?	synthetic incident drill and recovery note
Remediation	Which wording, workflow, source, figure, or assessment gate must change before reuse?	owner, due date, retest result, and refresh trigger

2.24 Model and dataset documentation card: intended use, provenance, caveats, and lifecycle

Field	Model card evidence	Dataset card evidence	Review gate
Intended use	accountable task, excluded uses, affected users, human reviewer, and accountable owner	Data Cards purpose statement, recommended use, prohibited reuse, stewardship owner, and affected stakeholder groups	claim is rejected if intended use, excluded use, affected users, or owner is missing
Provenance and collection	model family, version, supplier or lab, training cutoff, deployment context, and configuration hash	upstream source, collection process, annotation method, consent or authority basis, sensitivity class, and license	artifact is held if provenance, license, authority, or collection process is opaque
Composition and limits	capability boundary, known failure modes, tool permissions, context window limits, and unsupported conditions	population, sampling frame, coverage gaps, subgroup visibility, missingness, transformations, and known caveats	artifact is revised if population, coverage, or source limits are invisible
Evaluation and caveats	benchmark suite, task-specific tests, subgroup or context results, red-team findings, uncertainty notes, and failure examples	quality tests, label agreement, bias review, measurement limits, transformation log, and Data Cards answer-evaluation notes	empirical or performance claims are rejected unless test context, subgroup caveats, and uncertainty are visible
Lifecycle controls	release gate, rollback path, monitoring signal, incident threshold, refresh trigger, and model-card update owner	retention rule, access boundary, update cadence, deletion path, stewardship handoff, and dataset-card revision trigger	reuse is blocked without owner, retention, monitoring, rollback, and refresh evidence

2.25 Transparency and communication notice: purpose, safeguards, human review, and limits

Step	Artifact	Review gate
Public purpose	plain-language purpose, authority, affected service, and decision role	reader can tell why the system exists and where human judgment remains
Tool and data summary	model, data, supplier, provenance, validation, and accessibility summary	sensitive details are de-sensitized without hiding accountability fields
Impact and review	benefits, risks, safeguards, human review, appeal, and contact point	affected groups can identify recourse and oversight owners
Publication decision	publish, partially publish, delay, or hold decision with exemption rationale	non-public fields have a documented legal, security, privacy, or IP basis

2.26 Records retention and audit trail: owners, retention rules, and deletion conditions

Record	Retained fields	Audit question
Source and prompt register	source identity, prompt version, tool allowlist, reviewer, timestamp, and caveat	Can a later reviewer reconstruct the evidentiary path without private or live data?
Decision and exception log	risk owner, accepted exception, compensating control, expiry date, and approval	Is every deviation time-bound, justified, and reviewable?
Artifact retention note	output type, sensitivity, access boundary, deletion rule, and refresh trigger	Does the retention choice match the educational purpose and rights impact?
Incident and remediation record	incident signal, containment action, root cause, owner, retest result, and closure date	Can the same failure be detected and prevented in the next reuse cycle?

2.27 Release and change-control gate: reuse approval, rollback, and change evidence

Gate	Release evidence	Block condition
Scope freeze	accountable use case, excluded actions, tool profile, and data boundary	scope expands to external action, live data, or an unreviewed capability
Security and rights review	privacy, accessibility, security, bias, and human-review checks	rights impact, vulnerability, or accessibility issue has no owner
Version and rollback	model or prompt version, changelog, test fixture, and rollback path	change cannot be reproduced, compared, or reverted
Post-release monitoring	monitoring signal, incident threshold, refresh trigger, and owner	deployment or reuse occurs without logging and retest commitments

2.28 Risk exception and acceptance memo: residual risk, owner approval, and review clock

Field	Minimum content	Approval rule
Exception requested	what requirement cannot be met, why, affected groups, and duration	exception must be specific, time-bound, and tied to a compensating control
Risk basis	likelihood, impact, evidence, uncertainty, alternatives, and rejected options	unsupported confidence or missing alternatives returns the memo for revision
Compensating control	human review, monitoring, access limit, disclosure, remediation, and owner	control must reduce risk without creating an operational workaround
Expiry and retest	expiry date, retest condition, review cadence, and closure criteria	open-ended exceptions are rejected

2.29 Learner support and accommodation plan: support rows, access barriers, and escalation

Need	Support	Evidence
Access and modality	captions, alt text, keyboard path, plain-language summary, and structured tables	accessibility checklist, defect log, and retest result
Cognitive load	worked examples, staged release, glossary, checklist, and optional practice fixture	UDL design note and learner feedback record
Assessment fairness	allowed-tool statement, AI-use declaration, alternative submission mode, and transparent rubric	assessment-integrity note and accommodation record
Feedback and remediation	revision path, office-hour prompt, example correction, and due-date flexibility policy	feedback log and instructor disposition

2.30 Instructor question bank: prompts, evidence checks, and misconception probes

Question type	Prompt	Evidence
Source challenge	Which claim would fail if the strongest source were removed or downgraded?	claim ledger revision and source-lane note
Boundary challenge	Where could this exercise drift from analysis into action, and what safe substitute prevents it?	safe-substitution decision and excluded-action card
Rights challenge	Which affected group, accessibility need, privacy interest, or redress path is under-specified?	HRIA/DPIA update and accommodation note
Assurance challenge	What failure would the current evaluation miss, and what retest would reveal it?	adversarial assurance retest and remediation owner

2.31 Remediation backlog: issue owners, retest evidence, and closure boundaries

Backlog item	Trigger	Closure evidence
Unverified claim	claim lacks a guide citation or directly verified anchor	verified source, removed claim, or explicit source-guide context note
Unsafe phrasing	wording implies live targeting, external action, exploitation, manipulation, or unsafe control	safe substitute, blocked context, and reviewer sign-off
Accessibility defect	artifact cannot be inspected through an expected assistive or alternative workflow	defect fix, alternative means, and retest result
Assurance gap	evaluation, release, exception, incident, or vendor evidence is incomplete	owner, due date, retest, and accepted disposition

2.32 Scholarship and governance stance: source posture, claim limits, and public-readiness boundary

AGEINT treats agentic intelligence as a governed socio-technical practice, not as a bag of prompts or autonomous tricks. The curriculum therefore keeps AI agent evaluation, identity, authorization, secure tool use, structured analytic tradecraft, cognitive security, OSINT/GEOINT integrity, and ICS/OT safety in one source-backed frame. Each source anchor has a curriculum role, a domain, and a provenance type so readers can distinguish law, standards, official guidance, public-domain historical material, scholarly synthesis, and weaker practitioner or vendor context. Unless a section cites an empirical study or evaluation source for a narrower point, AGEINT language should be read as proposed design guidance and an assurance framework rather than measured performance evidence. Technical and theoretical analogies, including active-inference material, remain bounded by their direct domain sources and do not become deployment evidence without separate evaluation support.

The same stance now has a machine-checkable extension. Citation presence is necessary but not sufficient for AGEINT scholarship, so the generated manuscript is checked for source-family mix, uncited claim-bearing sections, thin claim-bearing support, and sections whose support comes from only one broad family. The audit distinguishes hard failures from review warnings: a claim-bearing overview, lesson, worked example, architecture source section, research-governance section, assessment review, or unit introduction with zero or one unique citation fails the current artifact evidence; a section with multiple citations from one source family is reported as a review target for future triangulation. The control surface is summarized in Figure 17, and the machine-readable companion report is written to `output/reports/scholarship_quality.json` during the current-evidence pass. This keeps source-guide inheritance visible while still preferring official, standards, law/policy, public-domain, and scholarly anchors whenever a section makes a stronger governance, technical, or empirical claim [Melissa L. Rethlefsen and the PRISMA-S Group, 2021]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d].

Claim calibration sits beside that scholarship audit. The source-strength layer classifies source-guide rows and curated anchors by whether they can carry a bounded claim directly or only provide context. Weak source-guide context, vendor/practitioner commentary, social/video rows, and mirror/copy rows cannot alone support empirical performance, statistical, governance-authority, safety, or formalism claims. The current report is written to `output/reports/claim_calibration.json` and `.md`, and the unified artifact evidence manifest exposes the result as `claim_calibration_ok`.

Analysis validation adds the reader-facing disposition layer, summarized as a claim-class-to-question matrix in Section 2.7 and Figure 20; that matrix is the boundary on what the manuscript can honestly say. This is why the artifact-evidence manifest records both positive counts and false-certification controls.

2.33 Verifier-first artifact evidence: build freshness, audits, and negative controls

AGEINT uses the RedTeam rule that a green validator is evidence only after the validator has been challenged. The artifact-evidence control loop in Figure 16 binds source-owned curriculum inputs, generated manuscript sections, citation inventories, figure metadata, PDF annotations, and current evidence reports into one falsifiable chain. This keeps scholarship, visual assets, and render validation in the same audit surface: a stale PDF, a local Markdown-file link, an uncovered source section, or a figure-registry mismatch must fail the evidence manifest before a maintainer can treat the render as ready. The same stance follows the evaluation and red-team assurance guidance already encoded in the bibliography atlas: adversarial testing is a scoped assurance method, not proof of universal safety or permission to run live operations [Cybersecurity and Agency, 2024a]; [of Standards and Technology, 2025a]; [of Standards and Technology, 2024e].

2.34 Orientation figures and course links: visual evidence, source flow, and navigation

The orientation uses Figure 5, Figure 6, Figure 7, Figure 8, Figure 9, Figure 10, Figure 11, Figure 12, Figure 13, Figure 14, Figure 15, Figure 16, Figure 17, Figure 18, Figure 19, Figure 20, Figure 21, Figure 22, Figure 23, Figure 24, Figure 25, Figure 26, Figure 27, Figure 28, and Figure 29 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.

Navigation links: Section 1, Section 3.

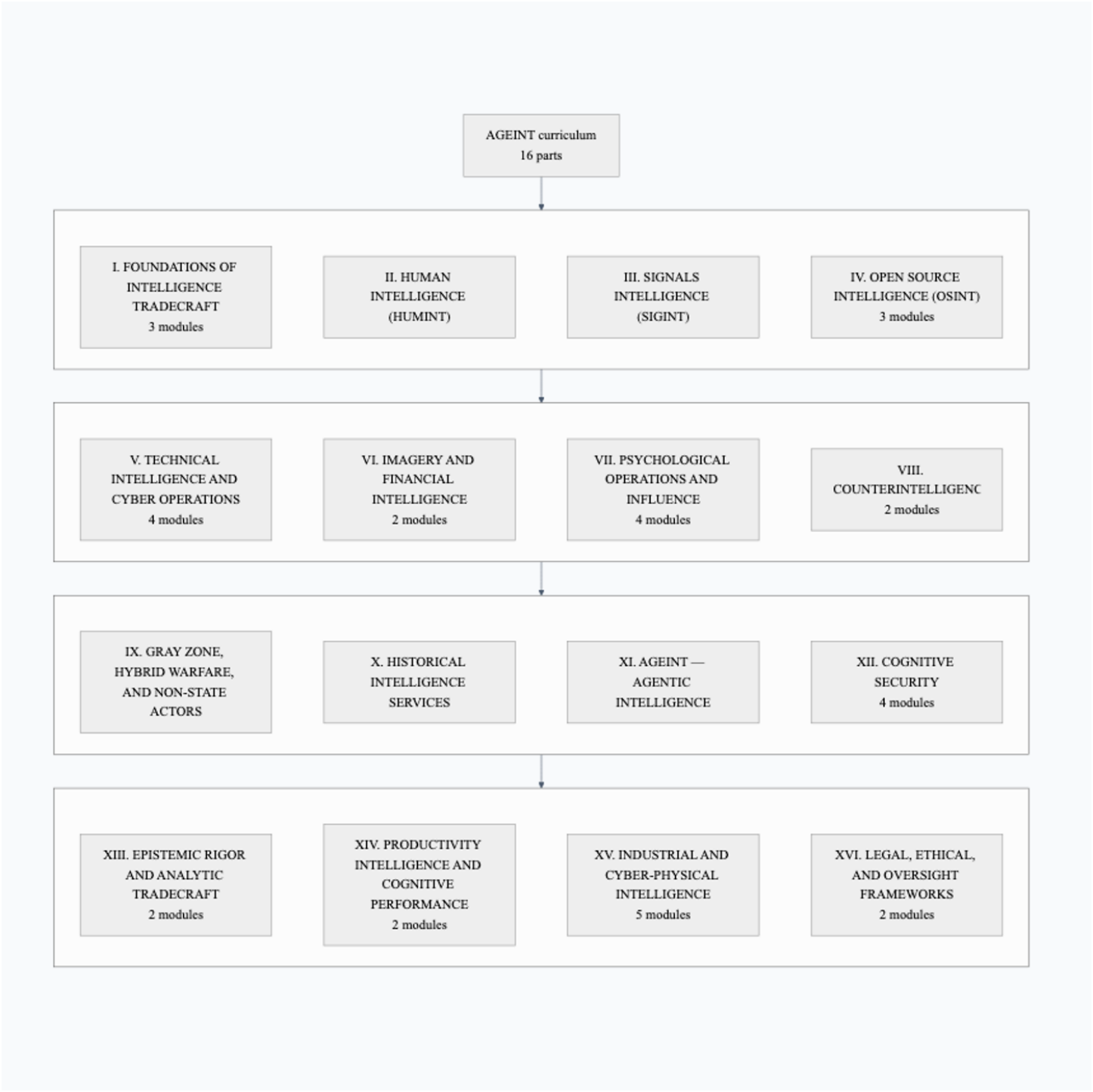


Figure 5: The curriculum map links AGEINT parts into a source-backed learning sequence. The captioned view belongs to the curriculum orientation and should be read as a map of 16 part nodes, source-backed module counts, and the reading path from tradecraft foundations through oversight frameworks, not as a capability score or live-task instruction.

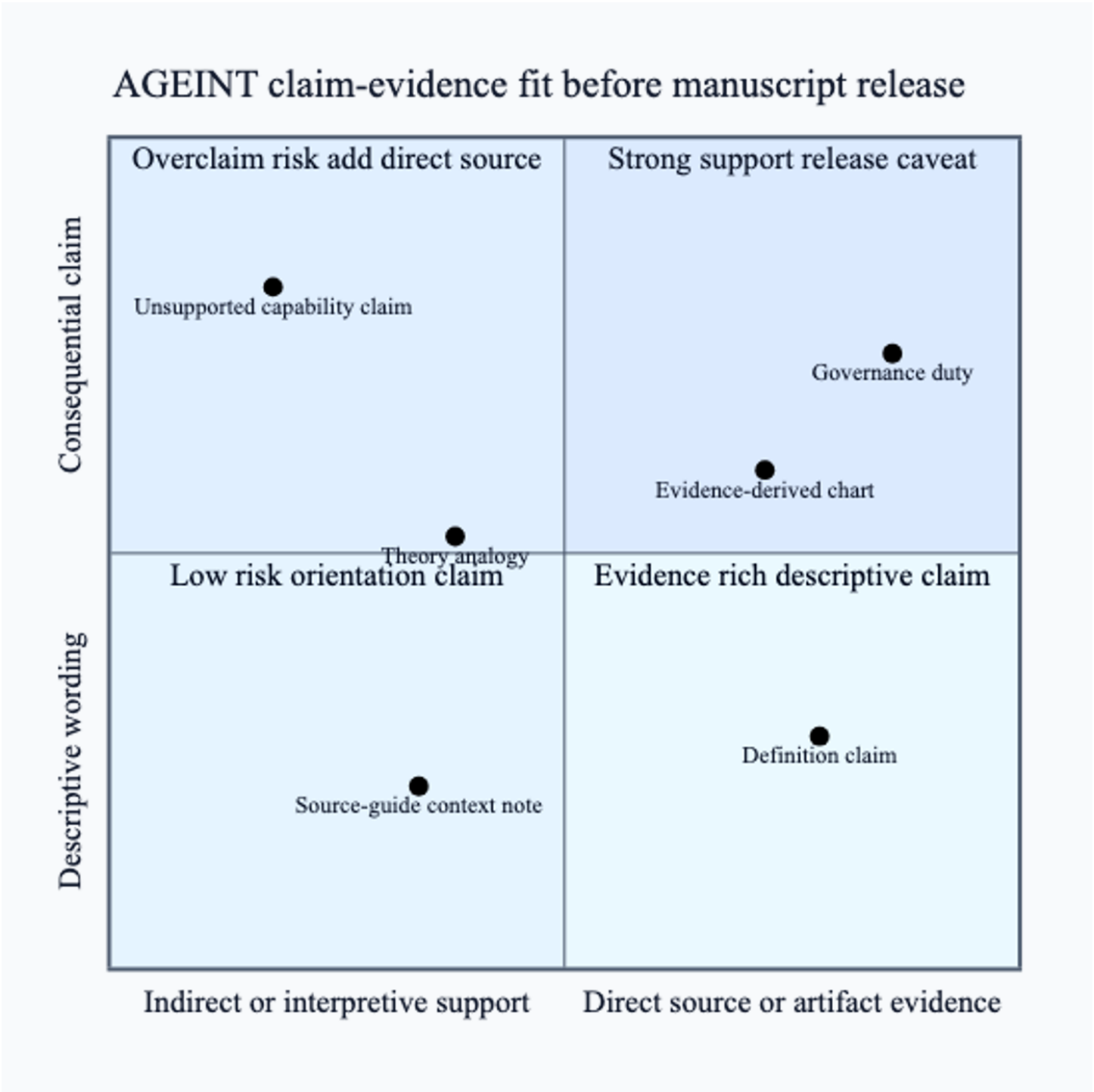


Figure 6: The claim-evidence quadrant helps reviewers distinguish low-risk definitional claims, governance duties, artifact-derived evidence, and high-caveat theory analogies before a manuscript sentence is treated as reviewable. Its reader value is to make x-axis evidence directness from indirect to direct, y-axis claim strength from descriptive to consequential, definition claims fit official or standard sources, and governance duties require policy or law text visible at a glance, with the curriculum orientation as the source section and defensive review as the boundary.

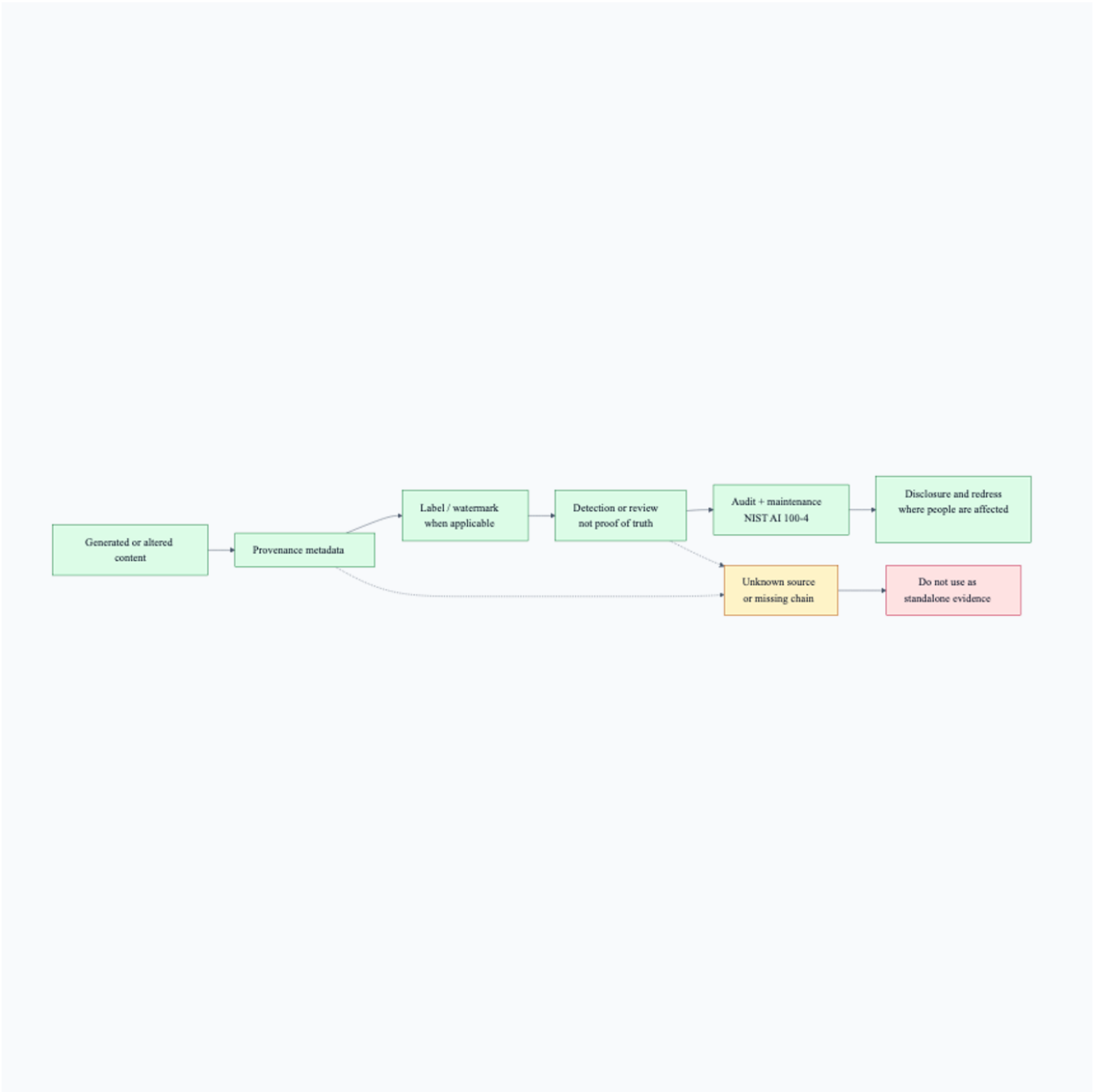


Figure 7: Source-backed conceptual schematic using NIST AI 100-4 to separate provenance, labeling, detection, testing, audit, and redress duties for generated visual and media claims. The captioned view belongs to the curriculum orientation and should be read as a map of Generated or altered content, Provenance metadata, Label / watermark when applicable, and Detection or review not proof of truth, not as a capability score or live-task instruction.

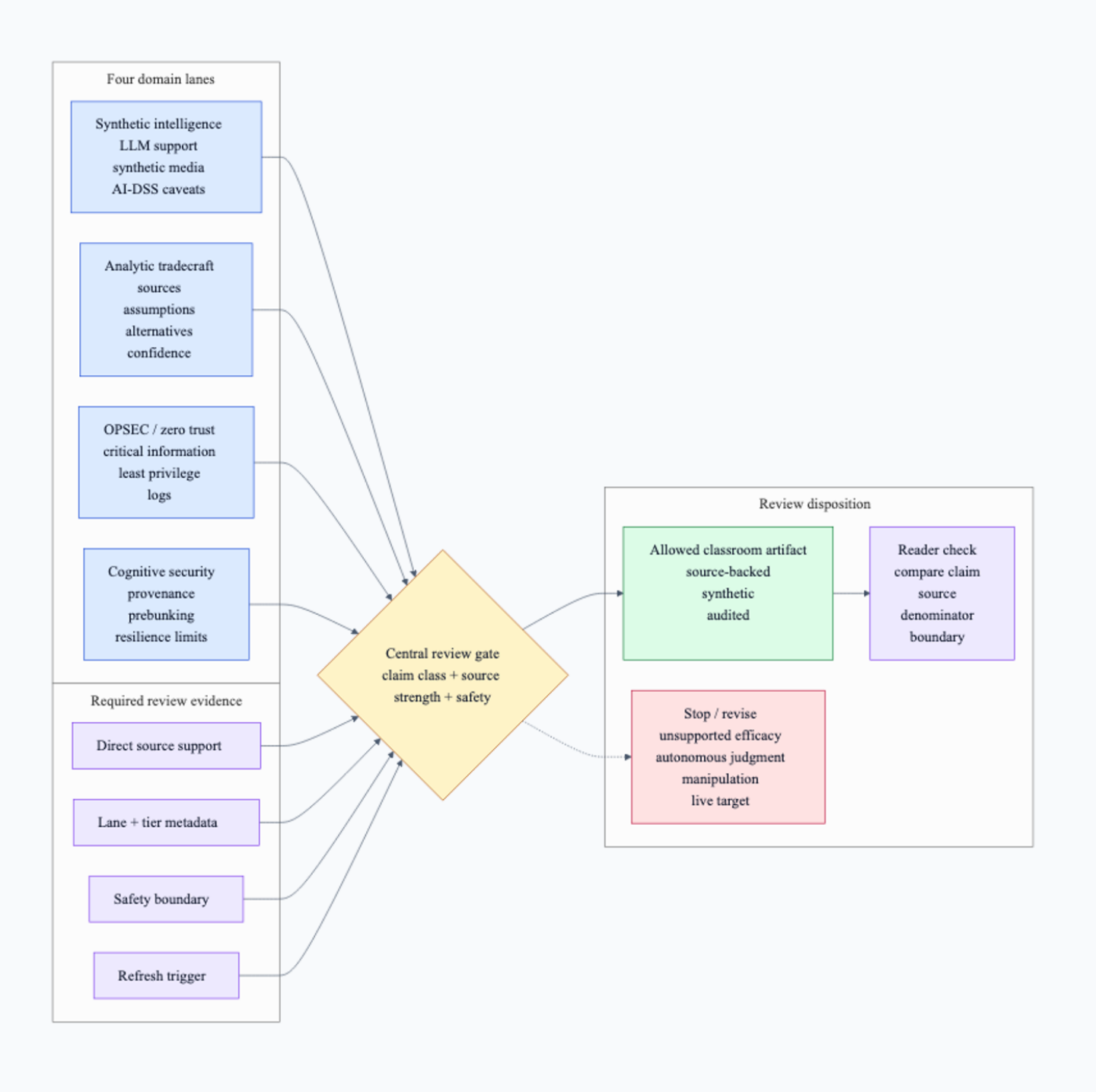


Figure 8: Source-backed architecture map showing four separate review lanes for synthetic intelligence, analytic tradecraft, OPSEC and zero-trust controls, and cognitive-security safeguards. The central gate requires direct source support, metadata, refresh evidence, and safety-boundary evidence before an allowed classroom artifact can be treated as source-backed; unsupported efficacy, autonomous judgment, manipulation, or live-target claims must stop or be revised.

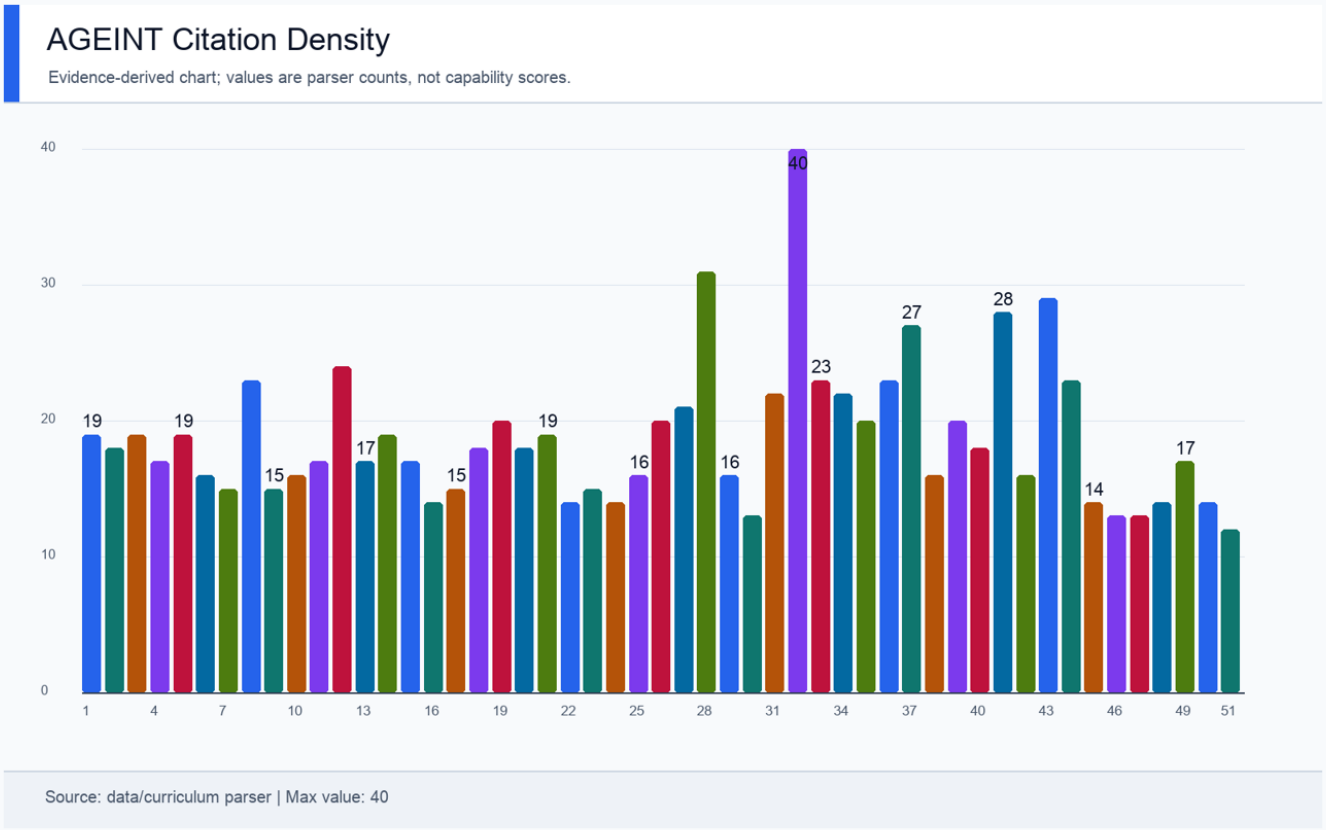


Figure 9: Method-backed audit chart reporting direct external citation counts per generated module; labels, denominators, and counting rule come from the curriculum parser. In the curriculum orientation, it lets readers compare citation density categories, denominators, evidence lanes, limitations, and reviewer-use cautions so the visual functions as a traceable course aid rather than an unscoped assertion.

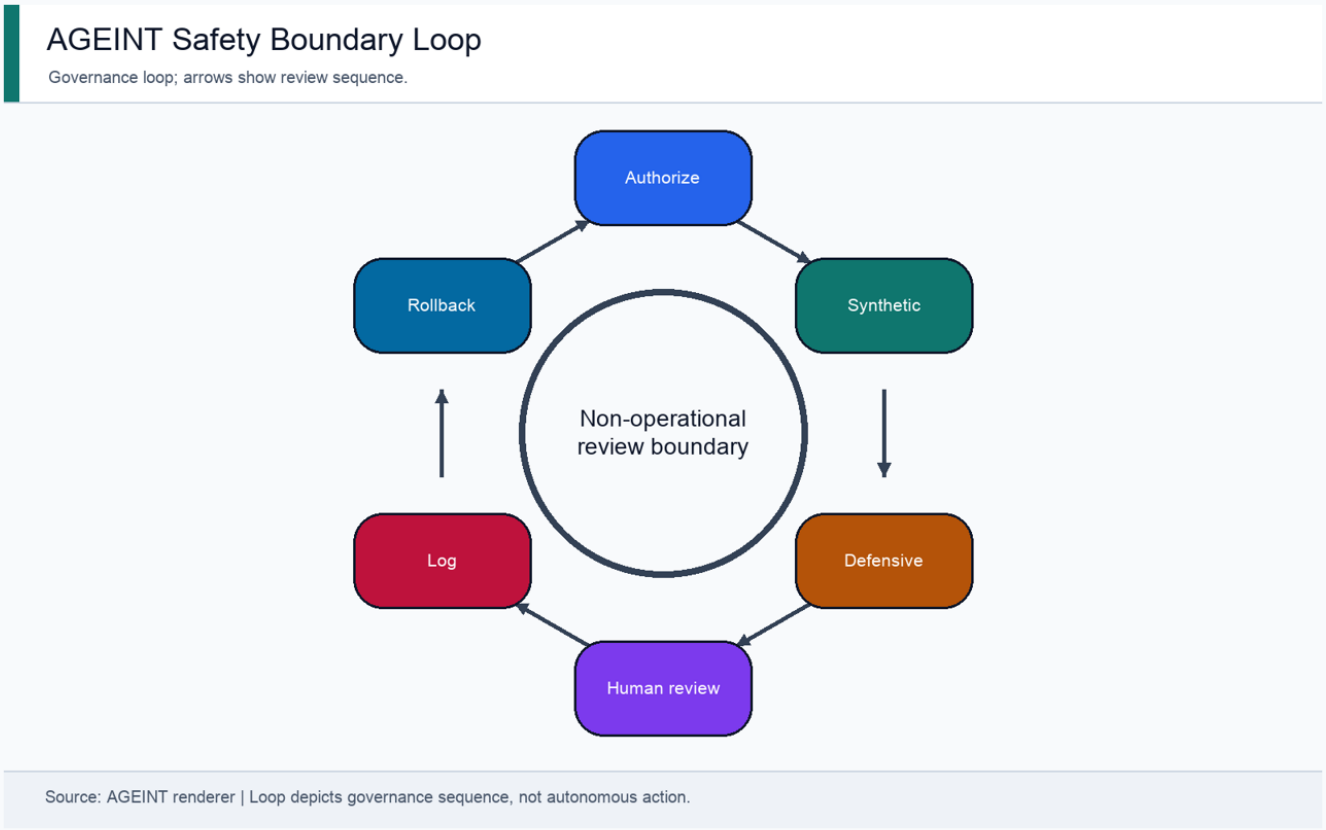


Figure 10: Conceptual governance schematic showing how accountable review, synthetic fixtures, human oversight, logging, and evidence-bounded practice stay connected. In the curriculum orientation, it lets readers compare safety boundary loop steps, decision gates, owner handoffs, refresh triggers, and closure evidence so the visual functions as a traceable course aid rather than an unscoped assertion.

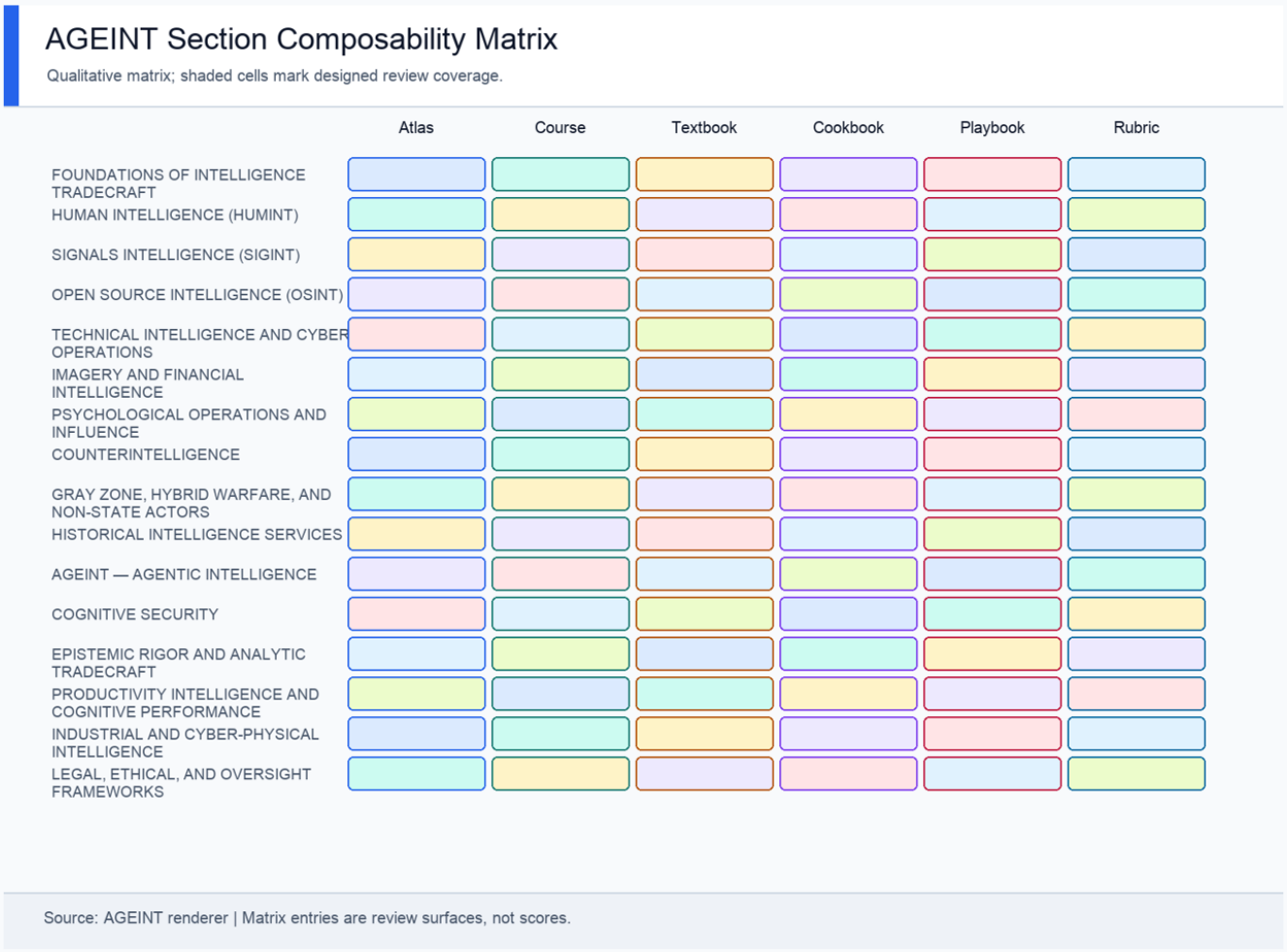


Figure 11: The section composability matrix shows which reusable curriculum artifacts support each part. It is anchored to the curriculum orientation; use it to inspect section composability matrix fields, row and column obligations, source records, reviewer decisions, and closure evidence while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

Figure 12: Conceptual compliance matrix with rows as governance lanes and columns as source, rights, assurance, artifact, and refresh obligations; color groups cells only. Its reader value is to make ai compliance map fields, row and column obligations, source records, reviewer decisions, and closure evidence visible at a glance, with the curriculum orientation as the source section and defensive review as the boundary.

Figure 13: The accessibility workflow joins WCAG, UDL, remediation, and refresh evidence. In the curriculum orientation, it lets readers compare accessibility workflow steps, decision gates, owner handoffs, refresh triggers, and closure evidence so the visual functions as a traceable course aid rather than an unscoped assertion.

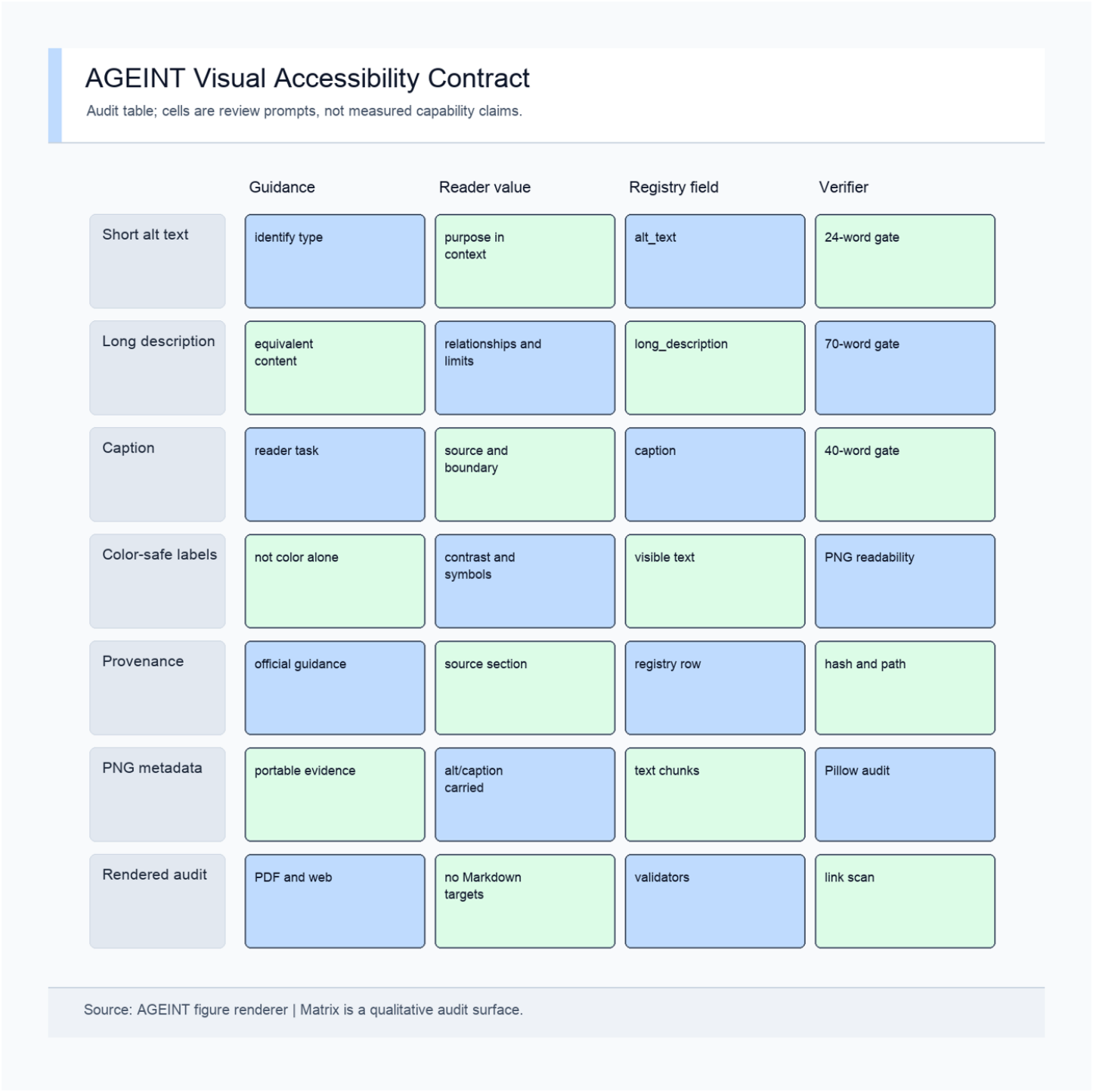


Figure 14: Source-backed accessibility contract mapping W3C WAI complex-image guidance, WCAG 2.2 non-text-content requirements, Section508 alternative-text and PDF checking guidance, and USWDS data-visualization guidance to AGEINT's generated figure registry. It shows how each figure carries a caption, short alt text, long description, source section, provenance, and rendered-artifact validation before PDF or web use.

Figure 15: Machine-checkable dashboard for the generated figure pipeline. It summarizes the quality gates that every AGEINT visual must pass: readable PNG assets, square-normalized layout, informative captions, short alt text, long descriptions, embedded PNG metadata, local provenance, and rendered-output link safety. The companion machine-readable artifact is `../figures/visual_quality_audit.json`.

Figure 16: Source-backed control-loop figure showing how AGEINT binds source-owned inputs, rebuilt manuscript files, citation inventory, figure registry metadata, PDF annotation audits, and current evidence reports so validators cannot certify a stale or partially copied artifact as complete. It is anchored to the curriculum orientation; use it to inspect artifact evidence control loop steps, decision gates, owner handoffs, refresh triggers, and closure evidence while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

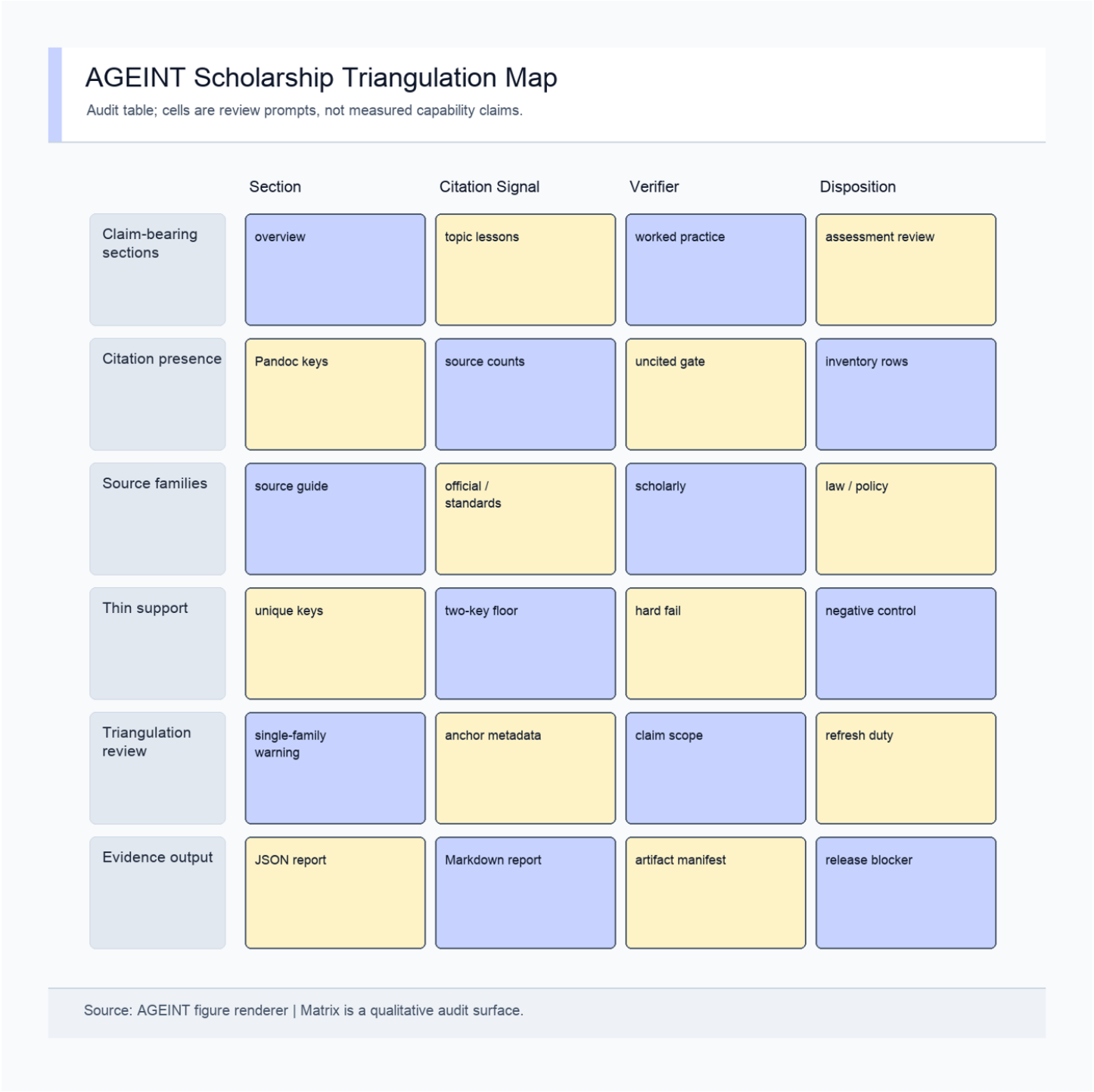


Figure 17: The scholarship triangulation map shows how generated AGEINT sections move from citation presence through source-family classification, thin-support gates, single-family review warnings, and current artifact-evidence reports. Its reader value is to make scholarship triangulation map fields, row and column obligations, source records, reviewer decisions, and closure evidence visible at a glance, with the curriculum orientation as the source section and defensive review as the boundary.

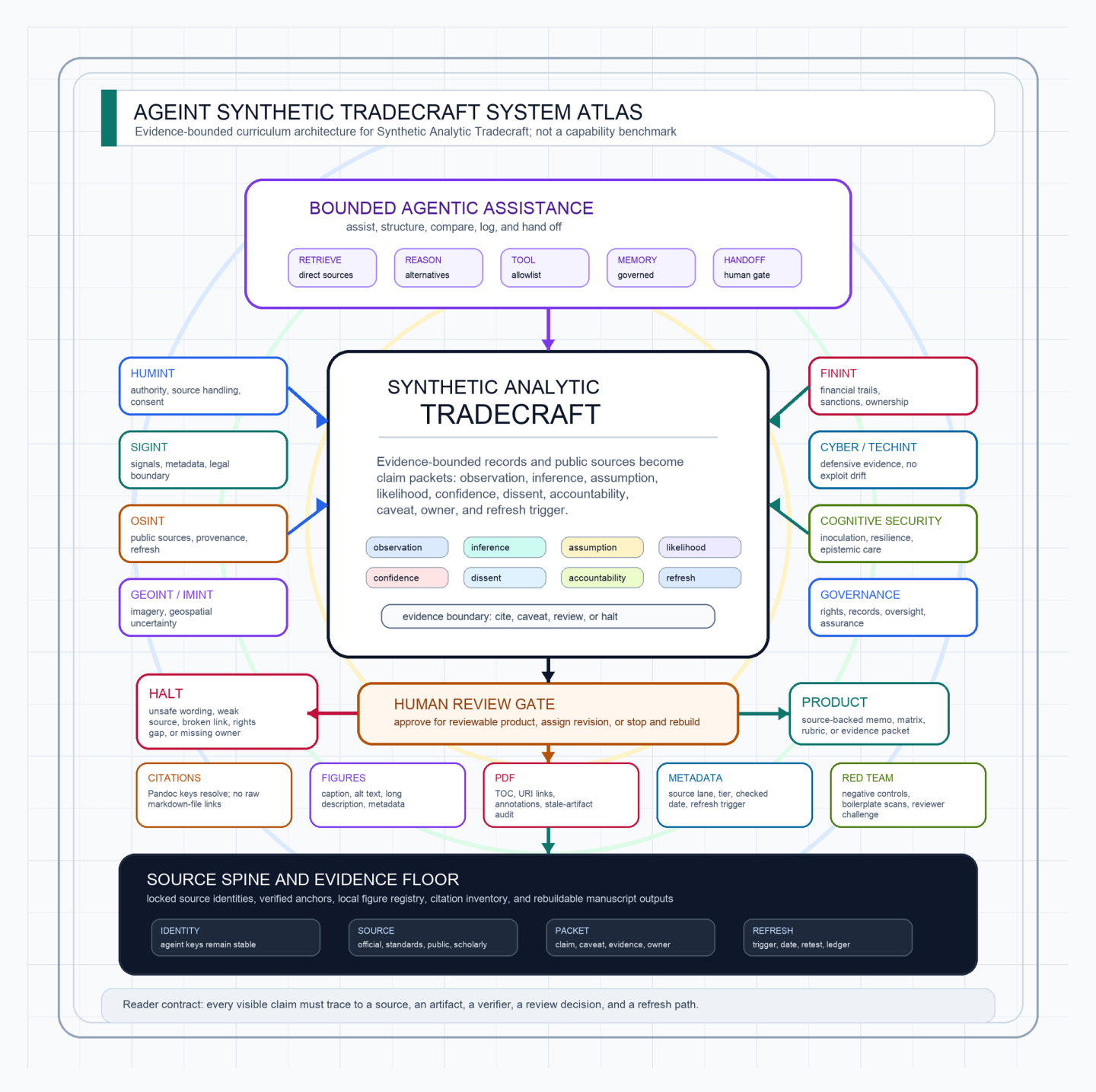


Figure 18: The Synthetic Tradecraft System Atlas replaces the former graphical abstract with a governed-system view of AGEINT. It shows the source spine as the evidence floor; intelligence disciplines as collection and context lanes; Synthetic Analytic Tradecraft as the central claim-making contract; bounded agentic assistance as a limited support layer; and verification, safety, and human-review gates as the outer assurance ring. The figure is a curriculum architecture map, not a claim that AGEINT has measured field capability or learning outcomes.

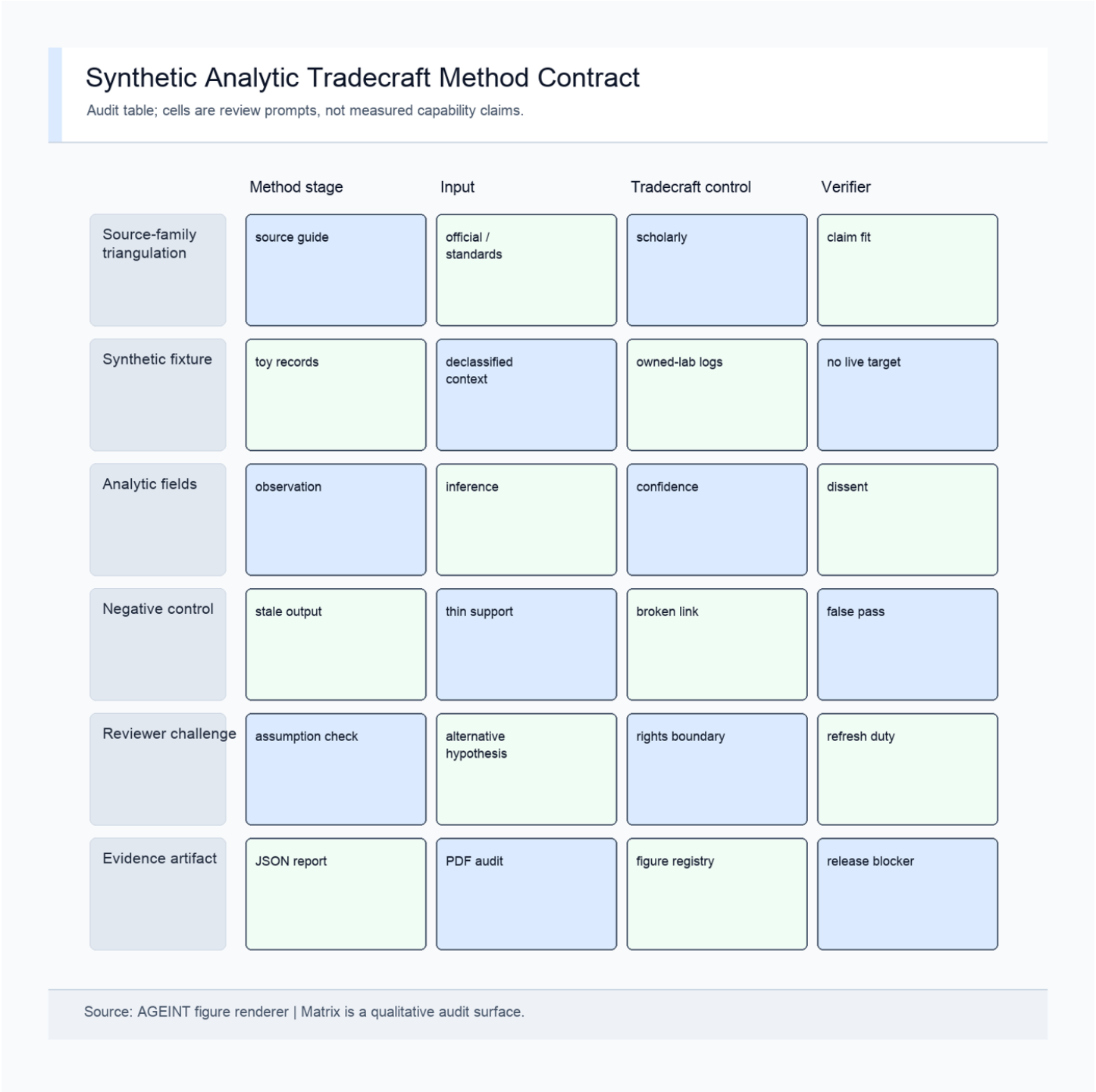


Figure 19: The method-contract figure makes AGEINT's Synthetic Analytic Tradecraft claim falsifiable. It links source-family triangulation, synthetic fixtures, analytic field separation, negative-control testing, reviewer challenge, and artifact-evidence reports so early manuscript claims remain method commitments rather than prestige language. Its reader value is to make synthetic tradecraft method contract labels, source records, review gates, refresh cues, and reader-use boundaries visible at a glance, with the curriculum orientation as the source section and defensive review as the boundary.

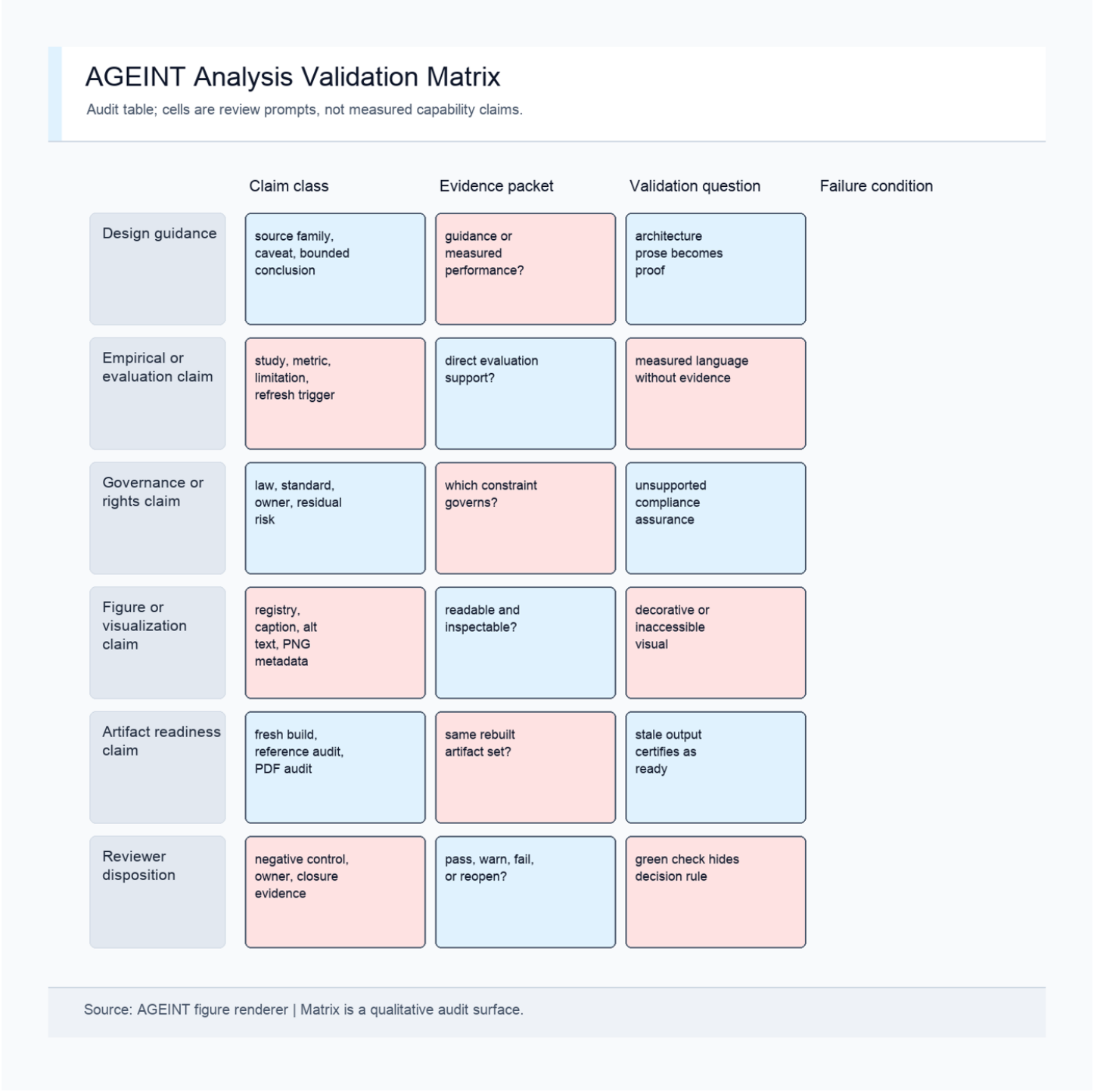


Figure 20: The analysis-validation matrix makes the manuscript's scholarship and assurance claims reviewable by class. It separates design guidance, empirical or evaluation claims, governance claims, figure/readability claims, rendered-artifact readiness claims, and reviewer disposition claims so each one has a required evidence packet, validation question, failure condition, and remediation path.

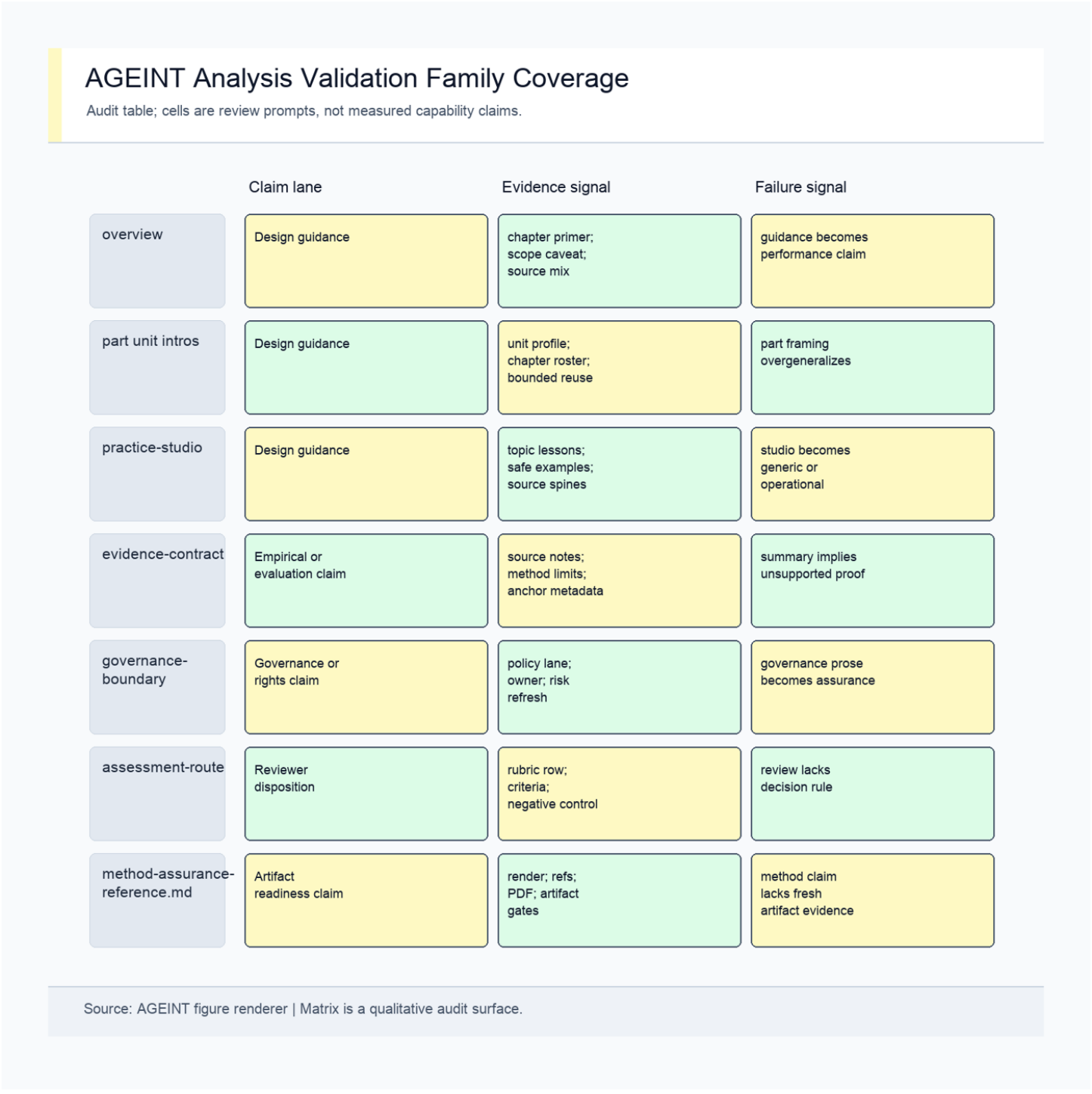


Figure 21: The analysis-validation family-coverage figure closes the gap between method prose and generated manuscript structure. It maps each claim-bearing manuscript family to a canonical analysis-validation lane, the evidence signal that should be present, and the failure signal that should block local readiness if a family becomes claim-bearing without a review class.

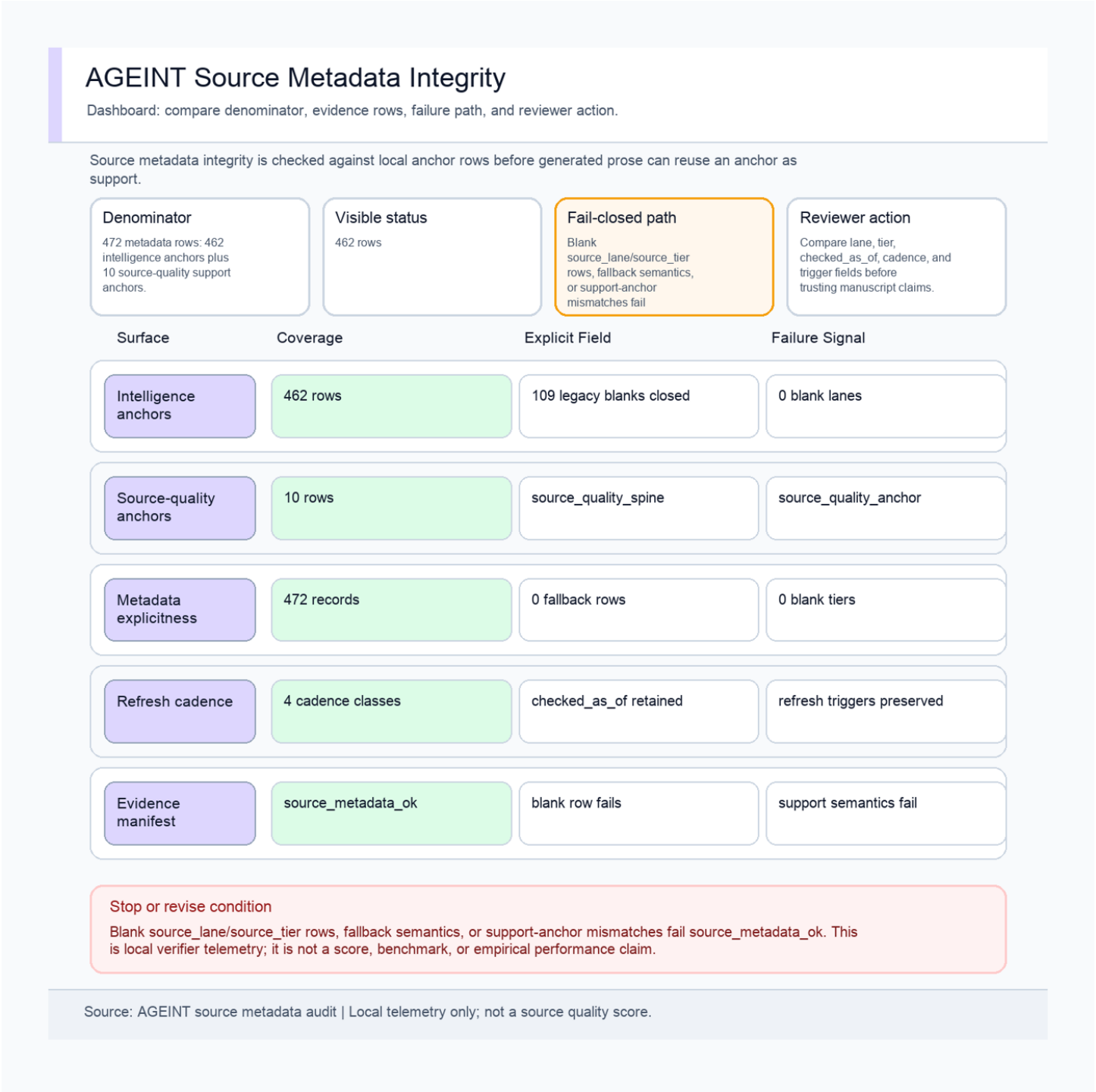


Figure 22: The source metadata integrity figure makes the anchor-lane hardening contract visible to reviewers. It separates curated intelligence anchors, source-quality support anchors, explicit lane and tier fields, refresh cadence evidence, denominator context, reviewer action, and the artifact-evidence manifest failure path so source rows cannot silently fall back to broad domain or source-type semantics while the rendered PDF still appears locally ready. Read it as local metadata telemetry, not a quality score for the cited sources.

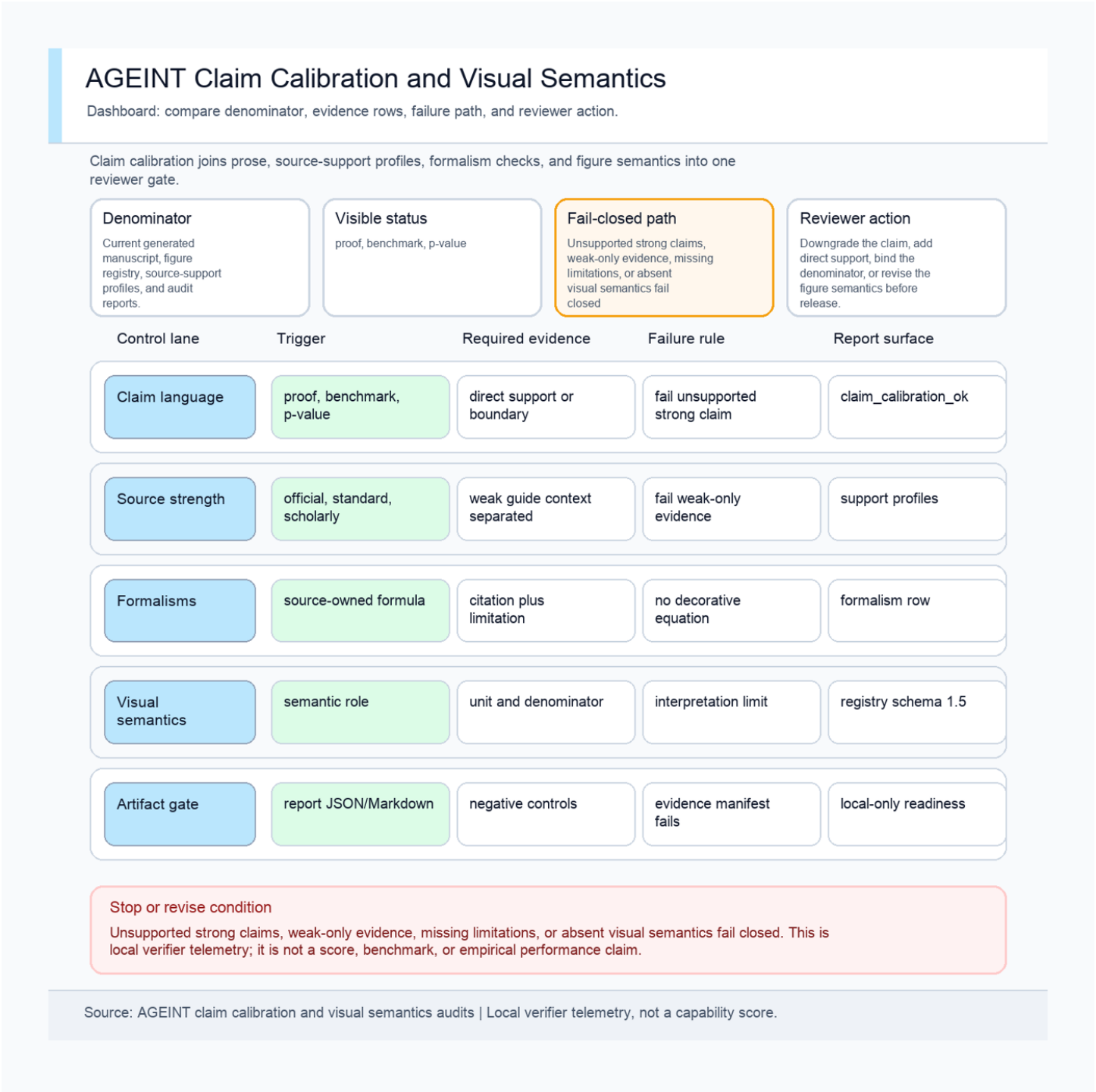


Figure 23: The claim-calibration verifier figure makes the final RedTeam/Science hardening layer visible: high-risk manuscript claims are separated into empirical, governance, visualization, artifact-readiness, safety, and formalism lanes; each lane must show direct support or explicit boundary language; weak source-guide context cannot carry measured-performance or statistical claims alone; and figure metadata must state semantic role, evidence role, quantitative status, denominator, counting rule, reviewer action, and interpretation limit before the artifact-evidence manifest can pass. Compare the local manuscript, registry, source-support, and report surfaces as reviewer inputs; do not read the visual as a score, benchmark, or empirical performance claim.

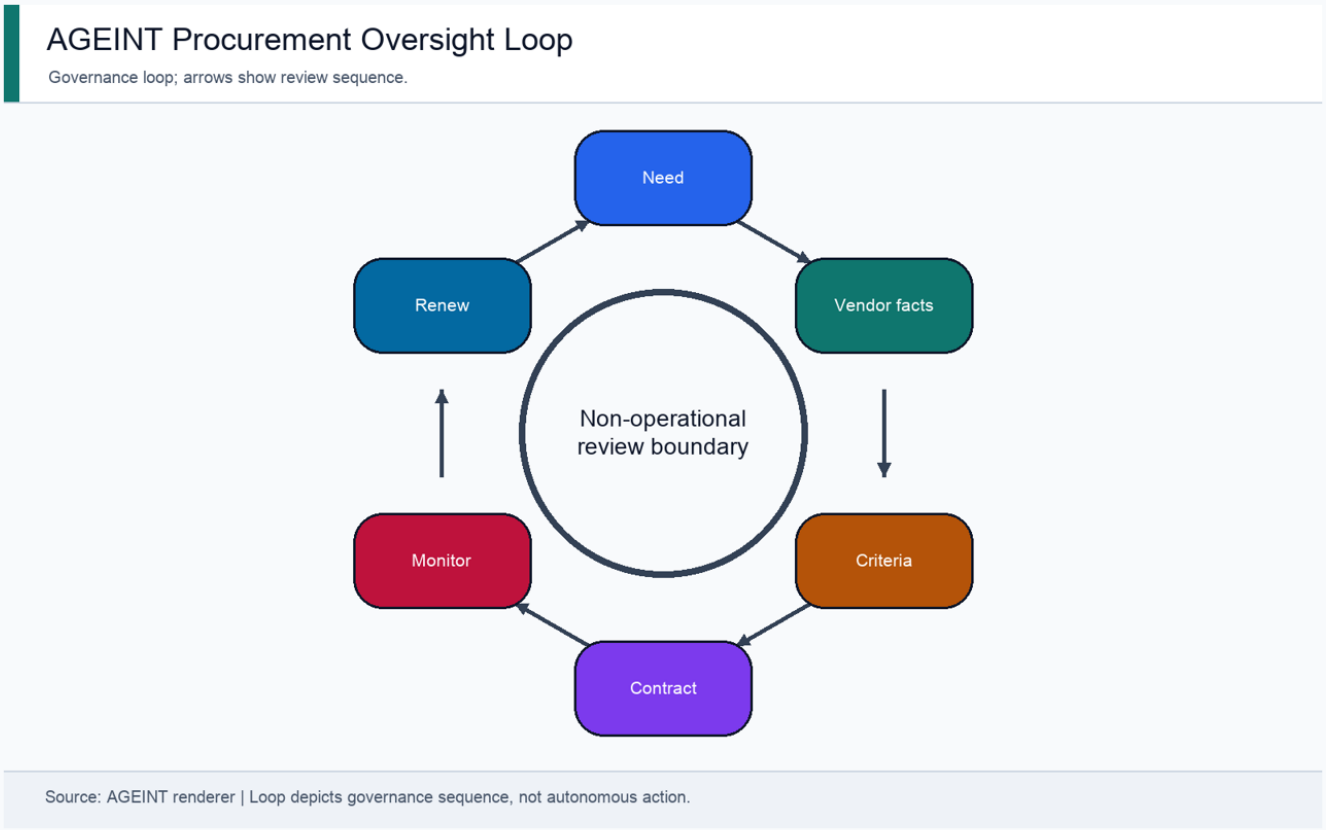


Figure 24: The procurement oversight loop connects need, transparency, criteria, contract controls, and lifecycle monitoring. It is anchored to the curriculum orientation; use it to inspect procurement oversight loop steps, decision gates, owner handoffs, refresh triggers, and closure evidence while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

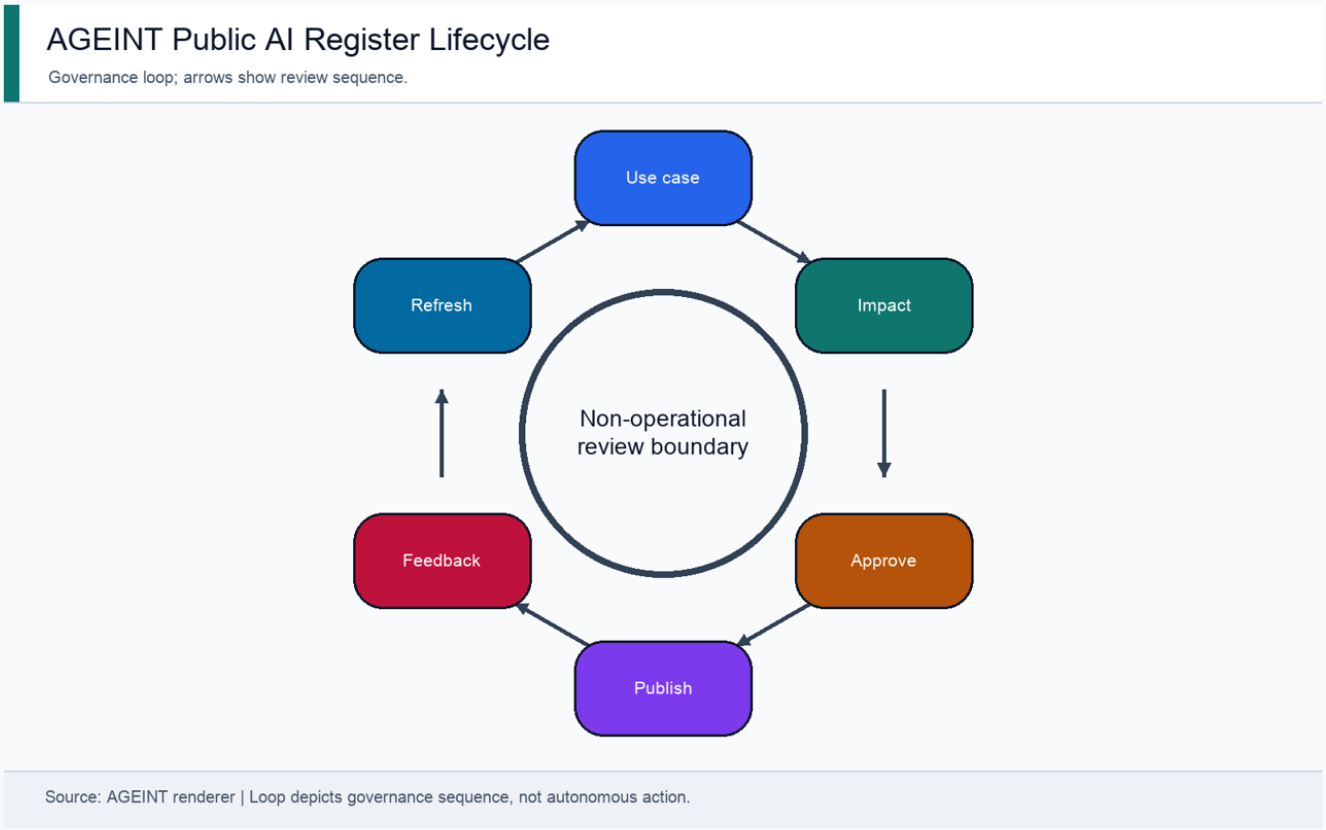


Figure 25: The public AI register lifecycle keeps use-case purpose, impact review, publication, feedback, and refresh visible. Its reader value is to make public ai register lifecycle steps, decision gates, owner handoffs, refresh triggers, and closure evidence visible at a glance, with the curriculum orientation as the source section and defensive review as the boundary.

Figure 26: The model and dataset card keeps purpose, provenance, collection process, evaluation caveats, lifecycle controls, and review ownership visible for model and dataset claims. It is anchored to the curriculum orientation; use it to inspect model dataset card fields, row and column obligations, source records, reviewer decisions, and closure evidence while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

Figure 27: The boundary-control matrix shows how purpose, tool permissions, data access, human review, logging, and rollback constrain agentic assistance before any external action can occur. In the curriculum orientation, it lets readers compare agentic intelligence boundary categories, denominators, evidence lanes, limitations, and reviewer-use cautions so the visual functions as a traceable course aid rather than an unscoped assertion.

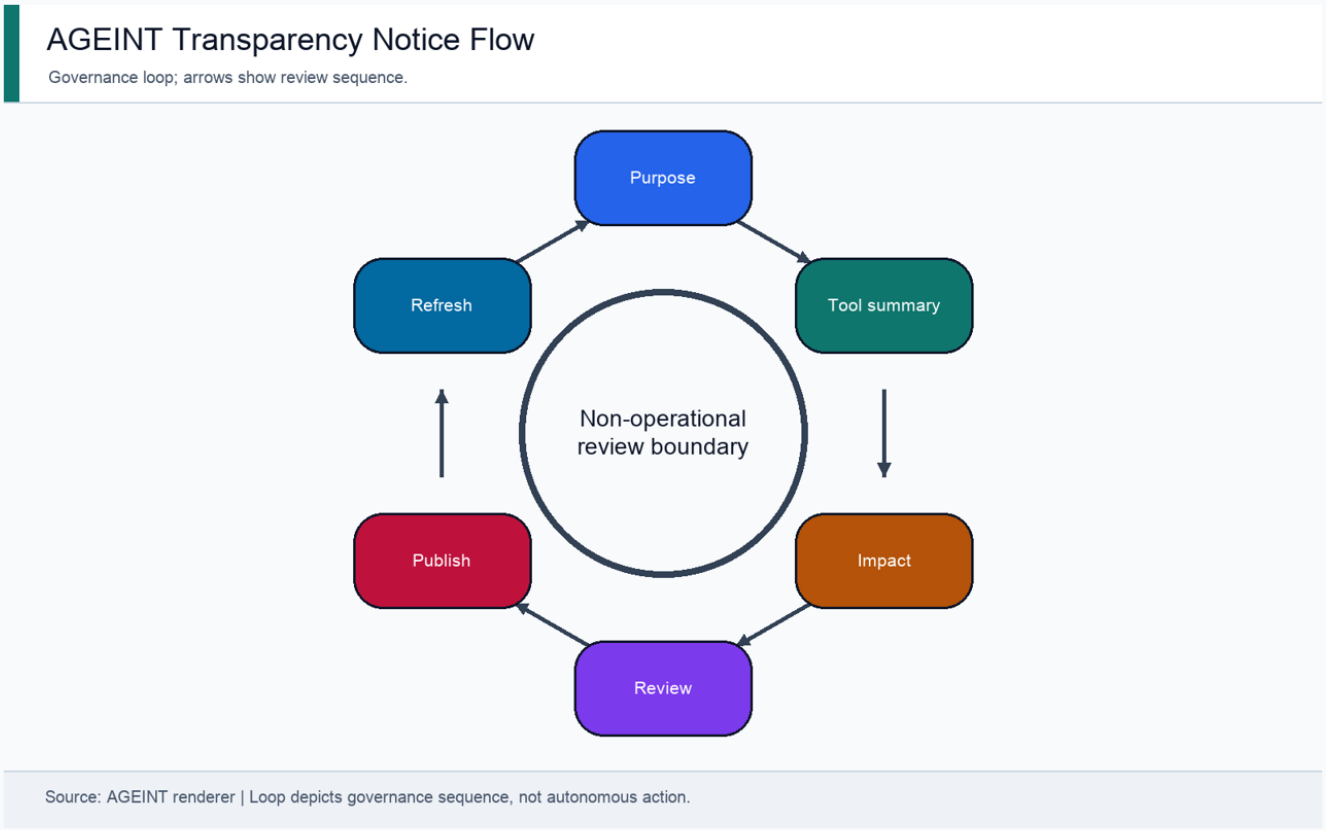


Figure 28: The transparency notice flow links public purpose, tool and data summary, impact review, and publication decisions. The captioned view belongs to the curriculum orientation and should be read as a map of transparency notice flow steps, decision gates, owner handoffs, refresh triggers, and closure evidence, not as a capability score or live-task instruction.

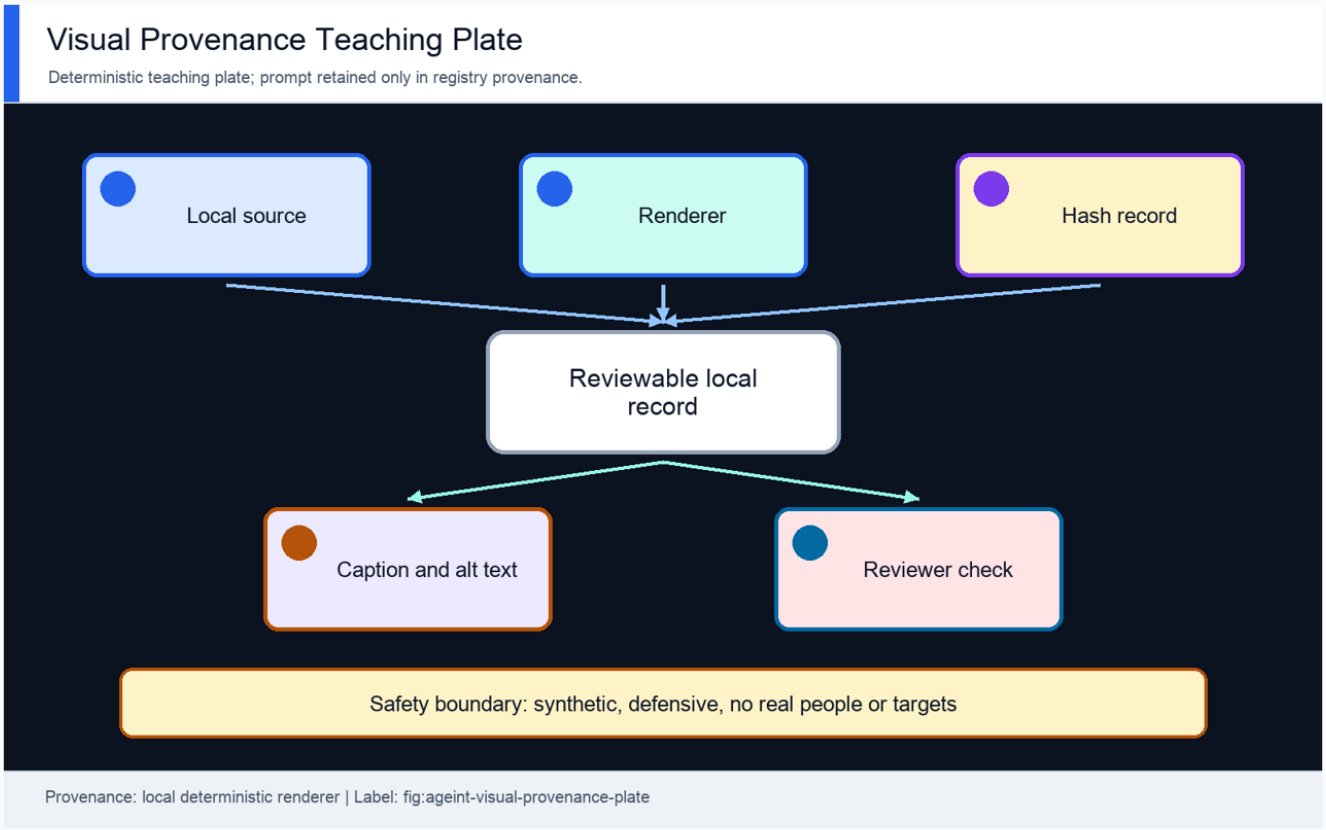


Figure 29: Deterministic teaching plate showing how AGEINT visual assets preserve local source, renderer, hash, caption, and review metadata before manuscript use. Its reader value is to make Local source, Renderer, Hash record, and Caption and alt text visible at a glance, with the curriculum orientation as the source section and defensive review as the boundary.

2.35 AGEINT pattern library: design-pattern rows, safe substitutions, and source identity

Source identity	Safe curriculum treatment	Methods	Defensive application	Safety boundary
Pattern 1: The Solo Reasoner (source identity only)	Focused Analytic Reasoner	bounded source reading, explicit assumptions, self-critique, and confidence notes	single public-source report critique with provenance and uncertainty fields	keeps reasoning reviewable without exposing hidden reasoning or delegating action
Pattern 2: The Reflection Agent (source identity only)	Reflection and Bias-Check Agent	rubric-based critique, source-quality scoring, and trajectory validation	analytic-bias review over a synthetic or public-source evidence packet	supports quality review and never replaces accountable human judgment
Pattern 3: The Tool-Forager (source identity only)	Tool-Allowlist Research Assistant	schema-bound tool calls, public-source retrieval, allowlisted connectors, and grounded summaries	accountable bibliography, source inventory, or standards-mapping exercise	excludes broad scraping, credentialed collection, and exposure-search tooling
Pattern 4: The Planner-Executor (source identity only)	Governed Planner-Executor	milestone decomposition, approval gates, dependency checks, and rollback notes	classroom project plan for evidence review, policy analysis, or tabletop preparation	plans curriculum artifacts only and does not create live operational tasking
Pattern 5: The Parallel Collector (source identity only)	Parallel Source-Corroboration Agent	bounded concurrent retrieval, deduplication, contradiction capture, and source descriptors	side-by-side comparison of public official, standards, and scholarly sources	uses public or provided materials and avoids intelligence collection expansion
Pattern 6: The Multi-Agent Crew (source identity only)	Role-Separated Review Crew	planner, retriever, validator, safety reviewer, and reporter roles	tabletop red-team critique of an analytic memo, not an operational exercise	keeps roles educational, logged, and constrained to benign artifacts
Pattern 7: The Debate Agent (source identity only)	Competing-Hypotheses Debate Agent	alternative generation, evidence challenge, dissent capture, and judge rubric	ACH-style review of a classroom claim with clearly separated evidence and judgment	does not generate adversarial persuasion or policy advocacy content
Pattern 8: The RAG-Operator (source identity only)	Provenance-Bound Retrieval Operator	curated corpus retrieval, hybrid ranking, source snippets, and citation audits	course-pack retrieval over provided readings, standards, and official guidance	does not connect to live sensitive stores or unapproved data collections
Pattern 9: The Memory-State Machine (source identity only)	Evidence-Memory State Machine	episodic note cards, retention limits, consolidation, and source change logs	longitudinal claim ledger for curriculum evidence and revision history	tracks claims and sources, not people, assets, or behavioral patterns
Pattern 10: The Control Plane Agent (source identity only)	Permissioned Control Plane Agent	single-interface routing, policy checks, budget limits, and audit logs	tool-governance demo that routes among benign summarization and validation utilities	keeps every tool revocable, observable, and constrained to evidence-bounded actions
Pattern 11: The Surveillance Agent (source identity only)	Monitoring-Governance Tabletop Agent	synthetic event polling, threshold rationale, alert review, and escalation logging	accountable monitoring governance exercise over toy asset-health records	prohibits tracking real people, real targets, private forums, or infrastructure
Pattern 12: The Red Team Agent (source identity only)	Control-Coverage Critique Agent	policy-safe scenario cards, control mapping, misuse-case review, and mitigation scoring	defensive tabletop review of controls against published high-level tactics	does not automate exploitation, weakness discovery, or attack-chain execution
Pattern 13: The Cover Story Generator (source identity only)	Identity-and-Provenance Fiction Audit	synthetic persona-risk critique, provenance labeling, and consistency-error detection	ethics exercise that detects fabricated identity artifacts in clearly synthetic materials	prohibits impersonation, false identity creation, and operational-security support
Pattern 14: The Deception Detector (source identity only)	Source-Reliability Verification Agent	corroboration, metadata review, provenance checks, and content-authenticity labels	public-source validation packet with uncertainty and review escalations	supports verification and does not accuse, deanonymize, or profile real people
Pattern 15: The Analyst in the Loop (source identity only)	Analyst-in-the-Loop Review Agent	interrupt gates, confidence thresholds, human approvals, and audit handoffs	supervised classroom analysis workflow for compliance-constrained exercises	requires accountable human review before any external communication or decision
Pattern 16: The Cyber Sentinel (source identity only)	SOC Tabletop Triage Agent	synthetic alert enrichment, ATT&CK mapping, severity rationale, and debrief notes	tier-1 incident tabletop over fabricated logs and published technique descriptions	does not run response actions, touch production systems, or publish indicators as fact
Pattern 17: The Supply Chain Inspector (source identity only)	Software Provenance Review Agent	SBOM reading, dependency graph review, advisory matching, and integrity questions	defensive package-governance exercise over sample manifests and public advisories	does not hunt real maintainers or produce exploitability claims without evidence
Pattern 18: The GEOINT Analyst (source identity only)	GEOINT Data-Quality Audit Agent	provided-image annotation, quality flags, geospatial metadata review, and caveat writing	synthetic imagery-change exercise focused on uncertainty and data quality	limits work to non-sensitive metadata quality, uncertainty notes, and synthetic location examples
Pattern 19: The Cognitive Inoculant (source identity only)	Cognitive-Resilience Education Agent	manipulation-technique labeling, transparent prebunking, and audience-harm review	opt-in media-literacy micro-lesson for a sample classroom scenario	does not design persuasion campaigns, microtargeting, or covert influence content

Source identity	Safe curriculum treatment	Methods	Defensive application	Safety boundary
Pattern 20: The Hierarchical Command (source identity only)	Hierarchical Curriculum Orchestrator	role delegation, output aggregation, exception routing, and failure recovery drills	multi-domain capstone coordination across benign module artifacts	orchestrates learning artifacts only and preserves human authorization gates

2.36 Safety rail: accountable, synthetic, defensive, and evidence-bounded boundaries

All exercises remain educational, lawful, defensive, historical, synthetic, and evidence-bounded. Modules may discuss intelligence, cyber, influence, counterintelligence, and industrial systems as objects of study, but they do not provide instructions for unauthorized collection, evasion, exploitation, manipulation, covert targeting, or real-world harm.

3 Method & Assurance Reference: claim evidence, safety gates, and refresh duties

This reference holds the shared method, governance, and assurance tables that every module applies. Each module links here instead of restamping the same tables, so a reader maintains one canonical copy of the capstone thread, claim ledger, competency rubric, refresh triggers, safety boundary, and mastery evidence. Module sections name their local source spine and topic, then point to the canonical table in this section.

3.1 Source-construction and reporting protocol: discovery records and citation boundaries

AGEINT is a curriculum-and-assurance atlas, not a PRISMA systematic review. Where a module makes a source-construction or literature-search claim, however, the source record follows PRISMA-S as a reporting discipline: record the discovery surface, search string or prompt, retrieval date, inclusion and exclusion rule, deduplication decision, source tier, conflict-handling note, direct URL, and refresh trigger [Melissa L. Rethlefsen and the PRISMA-S Group, 2021]. Discovery systems and summaries may suggest candidate sources, but final manuscript citations must resolve to directly checked official, standards, public-domain, or scholarly records in the AGEINT source atlas.

The review gate separates claim types before citation assignment. Governance claims require official or standards anchors; technical and theoretical claims require direct domain sources; empirical capability claims require evaluation or study evidence with context and subgroup caveats. If a source only supports an analogy, lesson design, or governance rationale, the generated prose must not promote it into a benchmark, deployment claim, or proof of autonomous performance.

3.2 Claim calibration and statistical limits: artifact telemetry versus empirical evidence

AGEINT treats citation counts, generated file counts, figure counts, PDF page counts, URI-link counts, and validator outcomes as **artifact telemetry**. They show what the local build produced and what the verifier checked; they are not learning-effect estimates, operational-performance measures, safety guarantees, or statistical evidence that the curriculum improves real-world analytic decisions. Stronger empirical or evaluated-capability language requires a direct benchmark, study, field evaluation, incident dataset, or scholarly empirical source with the method, denominator, subgroup/context caveat, and refresh trigger visible.

The claim-calibration audit enforces that separation after manuscript generation. It scans high-risk empirical, statistical, governance, safety, visualization, artifact-readiness, and formalism language; records the citation keys and source-support strength visible in the same row; allows explicit boundary language such as "not a benchmark" or "correct the misconception"; and fails unsupported proof-language, p-values, measured-performance claims, or formalisms without citations and limitations. The companion visual Figure 23 makes the control surface readable, while `output/reports/claim_calibration.json` and `.md` make the same disposition auditable by script.

Protocol claims are version-sensitive. MCP references use the 2025-06-18 specification for interoperability language and the current MCP security best-practice page for confused-deputy, token-handling, consent, and least-privilege examples; those claims must refresh when the protocol version, authorization profile, transport guidance, or security model changes [Project, 2025c]; [Project, 2025b]. Memory-language claims follow the same separation rule: MCP and official agentic-AI guidance support external-memory governance, tool boundaries, logging, and retention, not cognitive-taxonomy claims about episodic, semantic, or procedural memory unless a domain source is cited for that narrower taxonomy.

3.3 Method figures and course links: assurance visuals and navigation

The orientation uses Figure 10 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.

Navigation links: Section 2, Section 4.

3.4 Capstone phase, artifact, and review-gate ladder: required handoff sequence

Evidence anchor. Section 3; [Melissa L. Rethlefsen and the PRISMA-S Group, 2021].

Phase	Artifact	Review gate
Question	accountable learning question and excluded-action list	instructor confirms scope, allowed data, and rights impact
Source canon	source-lane map with guide citations, verified anchors, and refresh dates	citation keys resolve and source identity lock remains stable
Evidence ledger	claim, evidence, uncertainty, confidence, and reviewer register	every material claim has a source, caveat, and owner
Safe lab	synthetic or public dataset packet, tool allowlist, and stop conditions	no live target, private data, external action, or unsafe cyber-physical step
Assurance	evaluation rubric, failure-mode drill, rights map, and remediation note	human reviewer signs off before presentation or reuse
Debrief	capstone memo with lessons, residual risk, refresh triggers, and handoff owner	all unresolved questions and future approvals are explicit

3.5 Claim and evidence ledger: claim classes, evidence floors, and review duties

Evidence anchor. Section 3; [Melissa L. Rethlefsen and the PRISMA-S Group, 2021].

Claim class	Evidence required	Review gate
Source-spine claim	Parsed module title, module section map, and curriculum citation spine	Confirm the generated text does not invent counts, paths, or labels.
Research-backed governance claim	Direct official, standards, public-domain, or scholarly anchor in `references-*.bib`	Confirm the anchor has verification metadata and a stable URL.
Agentic workflow claim	Tool boundary, authority contract, human review point, and rollback condition	Confirm the workflow remains educational, logged, reversible, and evidence-bounded.
Technical or theoretical claim	Direct domain source for the formal expression, protocol, architecture, or theory, with analogy limits spelled out	Confirm the prose does not cite governance guidance as proof of technical performance or autonomous agency.
Empirical or evaluated capability claim	Direct benchmark, field evaluation, user study, incident evidence, or scholarly empirical source with context and subgroup caveats	Confirm the claim is not merely inferred from the AGEINT curriculum architecture.
Source-construction claim	Search surface, query or prompt, retrieval date, inclusion and exclusion rule, deduplication note, source tier, and direct URL	Confirm discovery sources are not treated as final citations unless directly verified.

Claim class	Evidence required	Review gate
Safety claim	Explicit prohibition plus safe alternative	Confirm the module blocks live targeting, exploitation, covert collection, manipulation, and unsafe cyber-physical action.
Cross-module claim	Link to the current unit and adjacent curriculum modules	Confirm the handoff names inputs, outputs, uncertainty, and next-review owner.

3.6 Competency and mastery rubric: scoring dimensions and visible proof

Evidence anchor. Section 3; [Melissa L. Rethlefsen and the PRISMA-S Group, 2021].

Competency	Evidence of mastery
Conceptual command	Terms are defined precisely and linked to the source spine.
Analytic rigor	Assumptions, uncertainty, alternatives, and confidence are explicit.
Agentic design	Human oversight, tool boundaries, logging, and rollback are specified.
Governance and rights	Authority, procurement, privacy, accessibility, retention, and redress evidence are visible.
Safety posture	Exercises remain accountable, synthetic, defensive, lawful, and evidence-bounded.

3.7 Refresh triggers and required actions: source, safety, and tool-change duties

Evidence anchor. Section 3; [Melissa L. Rethlefsen and the PRISMA-S Group, 2021].

Trigger	Required action
Source guide reference changes	preserve existing `ageintNNN` identities and append new references only after the locked range
Official or standards source updates	update source-lane metadata, checked date, and bibliography note
AI law, public-sector policy, education guidance, or rights guidance changes	rerun the compliance and rights map
API, protocol, data-space, or provenance specification changes	rerun interface and data-provenance checks
Safety audit finds operational wording	replace the treatment with tabletop, audit, governance, or synthetic-data framing
Instructor debrief finds unreproducible evidence	rebuild the source canon and claim ledger before reuse

3.8 Safety boundary: accountable, synthetic, defensive, and evidence-bounded practice

Evidence anchor. Section 3; [Melissa L. Rethlefsen and the PRISMA-S Group, 2021].

Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded. Do not convert any module into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action. Where a module inherits a risky source motif, treat it as a tabletop, audit, provenance, or governance exercise.

3.9 Mastery evidence standard: retained artifacts, reviewer challenge, and transfer

Evidence anchor. Section 3; [Melissa L. Rethlefsen and the PRISMA-S Group, 2021].

Level	Evidence in the answer
Strong	Uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary.
Adequate	Defines the concept and names a relevant artifact, but leaves one caveat or review owner vague.
Revise	Gives a memorized definition without source evidence, uncertainty, or a safe transfer task.

4 FOUNDATIONS OF INTELLIGENCE TRADECRAFT

4.1 FOUNDATIONS OF INTELLIGENCE TRADECRAFT learning spine and source route: unit purpose, module order, and evidence handoff

Evidence anchor. Section 4; [238, 2026].

4.1.1 intelligence-cycle governance discipline spine: domain question and learning focus

Evidence anchor. Section 4; [238, 2026].
This unit teaches **intelligence-cycle governance**. Requirements, collection, processing, analysis, dissemination, feedback, records, and oversight remain distinct so learners can see when research becomes intelligence work.

4.1.2 intelligence-cycle governance source-use contract: citation roles and evidence limits

Evidence anchor. Section 4; [238, 2026].
Use source-guide citations for inherited curriculum topics and official/standards anchors for claims about authority, quality, records, and review.

4.1.3 intelligence-cycle governance practice artifact: recurring packet and retained evidence

Evidence anchor. Section 4; [238, 2026].
The recurring practice artifact is a **requirements-to-product traceability ledger** that draws on requirement card, source descriptor, confidence statement, and dissemination and records note. The unit keeps its learning spine explicit. Learners translate a decision need into an accountable question, identify evidence channels, write confidence language, and preserve audit context.

4.1.4 intelligence-cycle governance safety boundary: accountable, synthetic, and evidence-bounded limits

Activities stay inside public, synthetic, or instructor-provided materials and never become live collection or tasking.
This unit introduces the part's governing question, evidence artifacts, source-support spine, and capstone thread before the individual modules begin. [238, 2026]; [237, 2026].
Learners carry one unit capstone thread through the part: define an accountable intelligence question, bind it to source-quality constraints, produce a reviewable artifact, test the artifact against failure modes, and hand it off with enough context for another analyst or instructor to audit. The capstone remains public, synthetic, or owned-lab throughout; its first source anchors are [238, 2026]; [237, 2026].
This unit's deliverables are a source-canon card, claim/evidence ledger, safe-practice lab packet, failure-mode note, instructor rubric, and debrief memo. The full source-lane and evidence-package ledgers appear in the orientation and appendices; this unit introduction keeps only the learner-facing spine for [238, 2026]; [237, 2026].
This unit's safety gates are scope authorization, rights review, data provenance, tool allowlisting, human oversight, rollback, and evidence-bounded output. A missing gate turns the activity into a tabletop, audit, or written governance exercise until the gate is restored against [238, 2026]; [237, 2026].
Capstone thread:

Phase	Artifact	Review gate
Question	accountable learning question and excluded-action list	instructor confirms scope, allowed data, and rights impact
Source canon	source-lane map with guide citations, verified anchors, and refresh dates	citation keys resolve and source identity lock remains stable
Evidence ledger	claim, evidence, uncertainty, confidence, and reviewer register	every material claim has a source, caveat, and owner
Safe lab	synthetic or public dataset packet, tool allowlist, and stop conditions	no live target, private data, external action, or unsafe cyber-physical step
Assurance	evaluation rubric, failure-mode drill, rights map, and remediation note	human reviewer signs off before presentation or reuse
Debrief	capstone memo with lessons, residual risk, refresh triggers, and handoff owner	all unresolved questions and future approvals are explicit

Research lane: Analytic Tradecraft and Source Integrity. Core anchors: [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2026e]. Conceptual focus: turning uncertainty into reviewable judgment through sourcing, alternatives, separated likelihood and confidence language, warning indicators, and explicit analytic lineage. Composability contract: every agent output must preserve evidence, assumptions, judgments, likelihood, confidence, dissent, empirical limits, and change history as separable fields. **Practice lens:** Structured-Judgment Lens; Which assumptions, alternatives, confidence statements, and source limits must stay visible for review? [238, 2026]; [237, 2026].

4.1.5 FOUNDATIONS OF INTELLIGENCE TRADECRAFT visual navigation and module map: evidence flow, order, and safety cues

The unit uses Figure 30, Figure 31, and Figure 32 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 3, Section 5.

4.1.6 FOUNDATIONS OF INTELLIGENCE TRADECRAFT module roster and source-lane inventory: citations, lanes, and learner route

Module	Section reference	Source spine
The Nature of Intelligence	Section 5	[238, 2026]; [237, 2026]; [270, 2026]; [273, 2026]; [274, 2026]; [275, 2026]; [286, 2026]; [287, 2026]; [292, 2026]; [001, 2026]; [002, 2026]; [003, 2026]; [004, 2026]; [005, 2026]; [297, 2026]; [298, 2026]; [309, 2026]; [310, 2026]; [300, 2026].

Module	Section reference	Source spine
Intelligence Community Architectures	Section 6	[234, 2026]; [247, 2026]; [249, 2026]; [276, 2026]; [277, 2026]; [284, 2026]; [288, 2026]; [289, 2026]; [293, 2026]; [006, 2026]; [007, 2026]; [008, 2026]; [009, 2026]; [010, 2026]; [011, 2026]; [012, 2026]; [297, 2026]; [298, 2026].
Tradecraft: Core Principles	Section 7	[237, 2026]; [266, 2026]; [269, 2026]; [278, 2026]; [279, 2026]; [283, 2026]; [290, 2026]; [291, 2026]; [294, 2026]; [013, 2026]; [014, 2026]; [015, 2026]; [016, 2026]; [017, 2026]; [018, 2026]; [005, 2026]; [019, 2026]; [297, 2026]; [298, 2026].

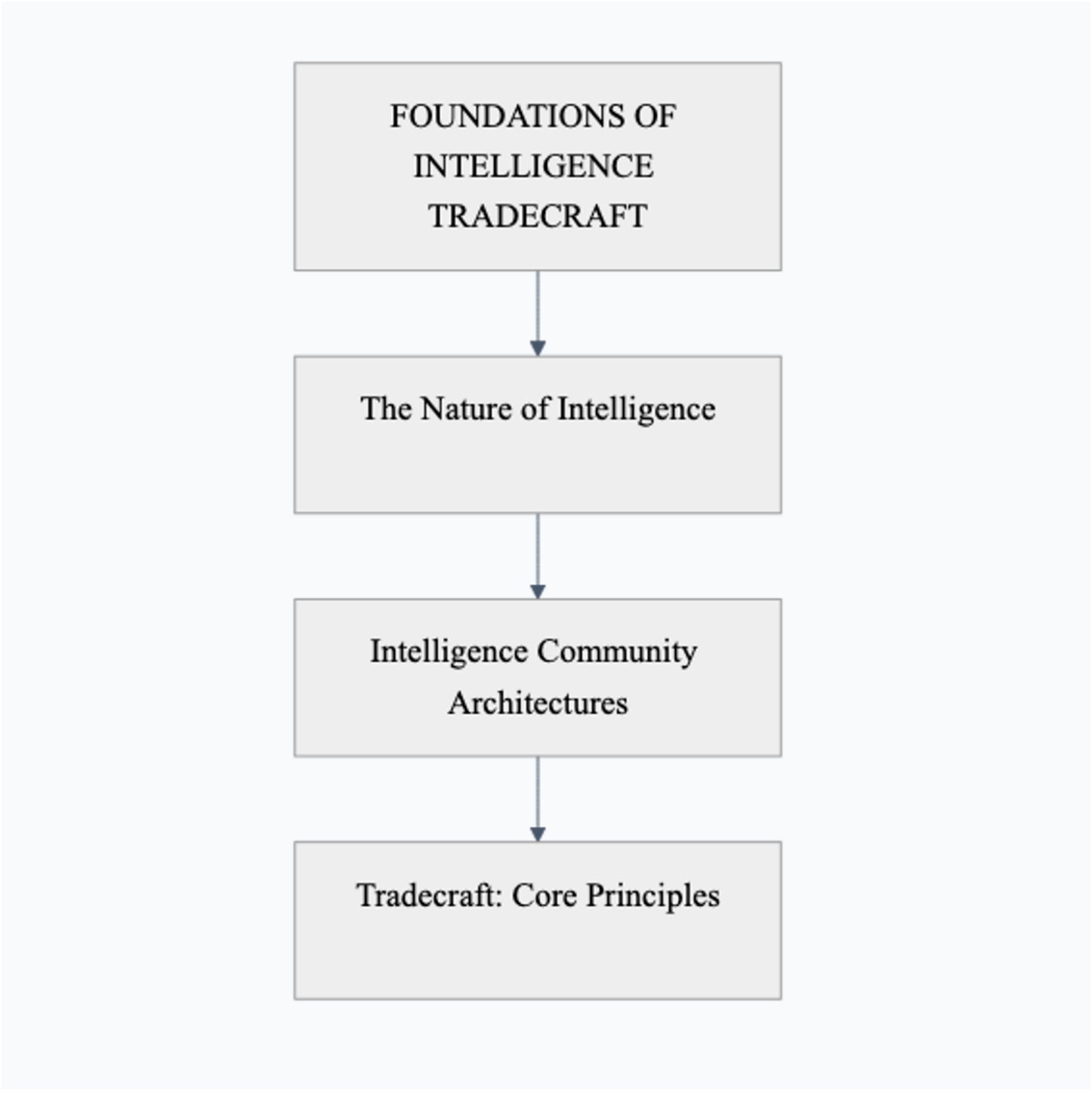


Figure 30: The unit module map traces the part's chapters as a linear reading sequence. The captioned view belongs to the foundations of intelligence tradecraft section and should be read as a map of 3 module nodes in the unit's ordered, source-backed reading sequence from its first module to its last, not as a capability score or live-task instruction.

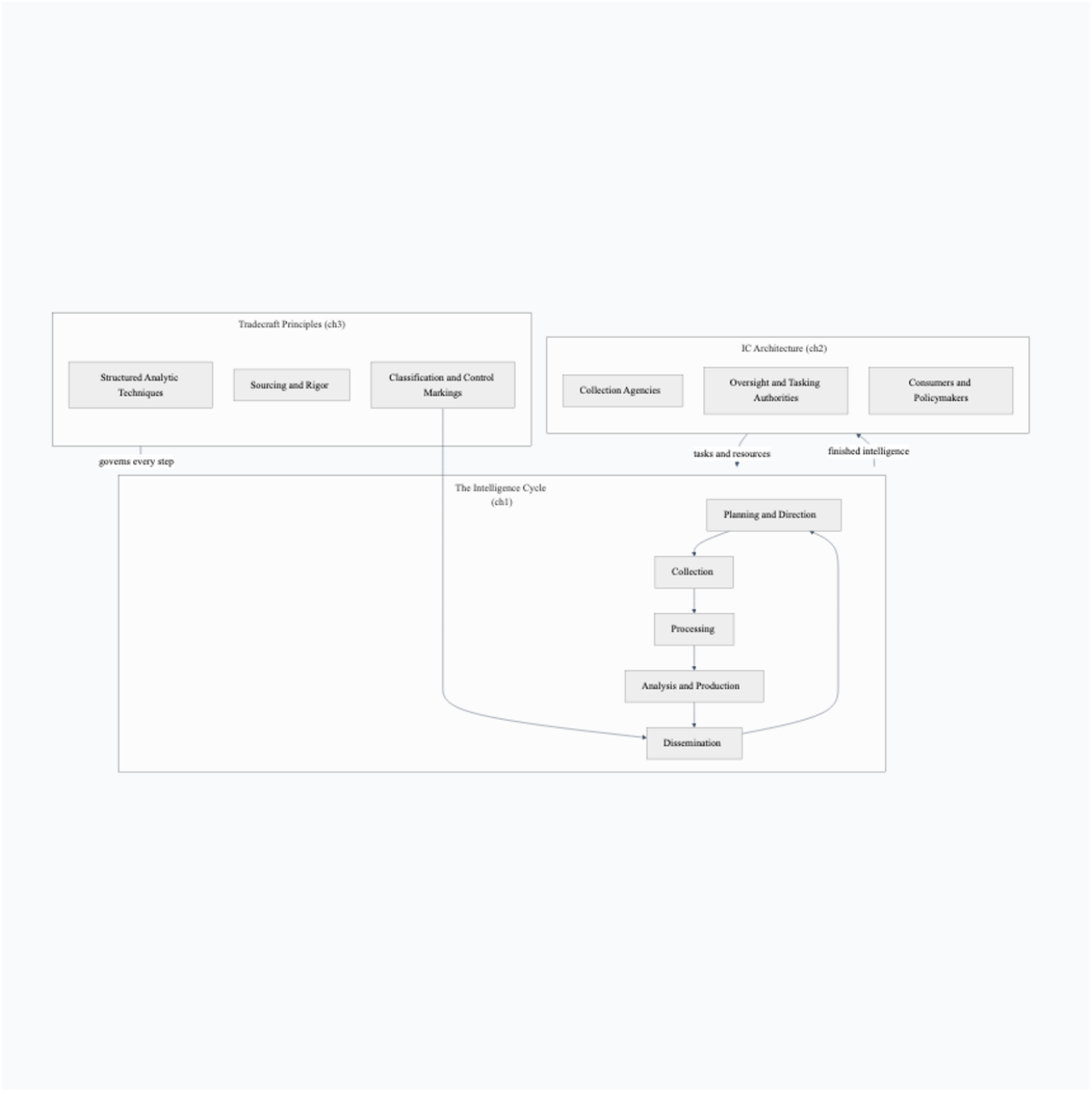


Figure 31: Part I frames intelligence as a cyclic process (ch1) driven by community architecture (ch2) and disciplined at every step by tradecraft principles and control markings (ch3). Its reader value is to make The Intelligence Cycle (ch1), Planning and Direction, Collection, and Processing visible at a glance, with the foundations of intelligence tradecraft section as the source section and defensive review as the boundary.

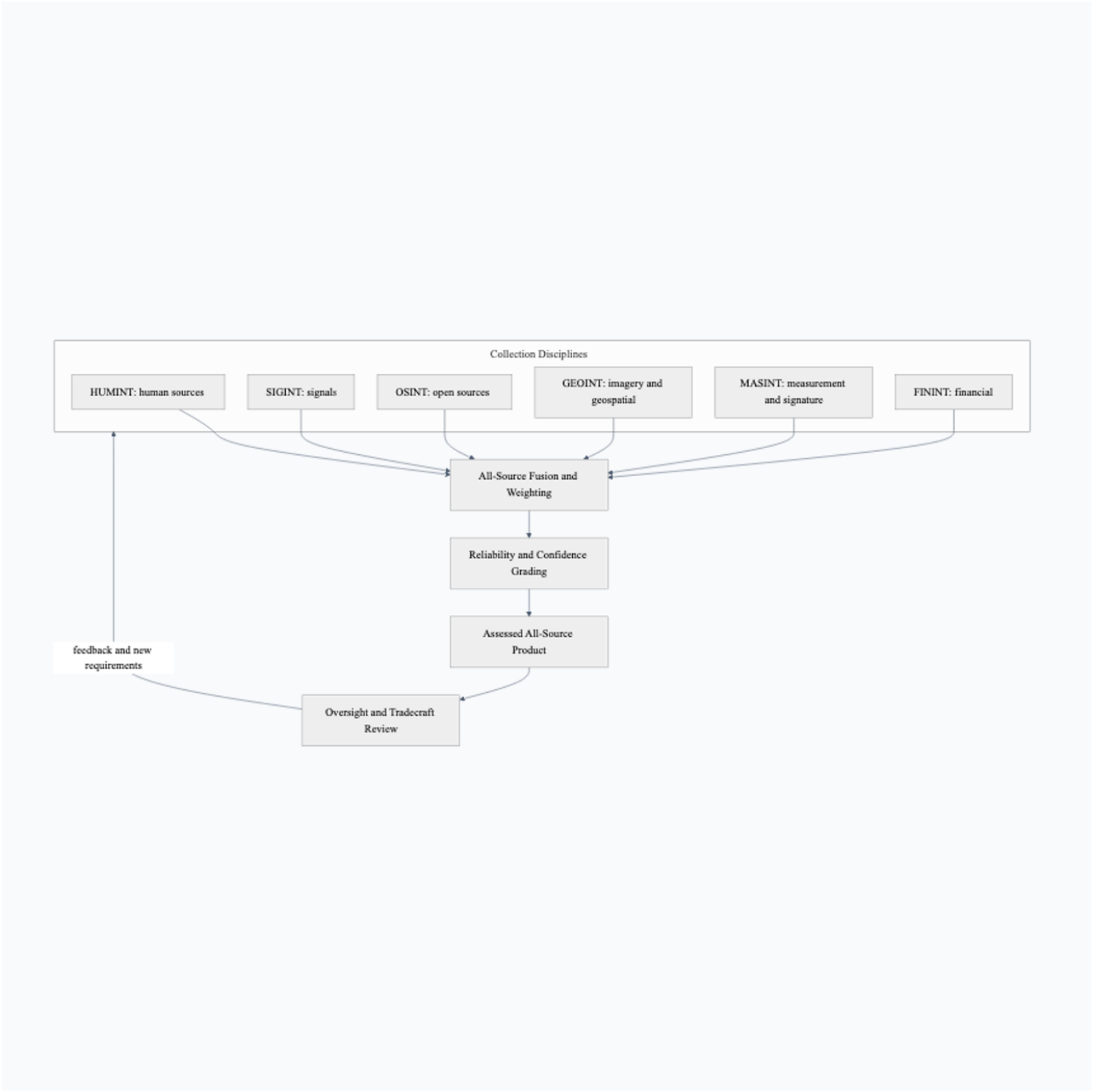


Figure 32: The intelligence disciplines each contribute distinct evidence that all-source analysis fuses, weights by reliability, and turns into an assessed product under oversight. In the foundations of intelligence tradecraft section, it lets readers compare Collection Disciplines, HUMINT: human sources, SIGINT: signals, and OSINT: open sources so the visual functions as a traceable course aid rather than an unscoped assertion.

5 The Nature of Intelligence

5.0.1 The Nature of Intelligence figures and course links: visual evidence, source flow, and navigation

The module uses Figure 33 and Figure 30 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 4, Section 6.
This module teaches the **Governed Intelligence Cycle and Dissemination Architecture** lane through a bounded, source-backed coursebook chapter. [238, 2026]; [237, 2026].

5.1 Governed Intelligence Cycle and Dissemination Architecture frame for The Nature of Intelligence: source context, topic focus, and reader task

Evidence anchor. Section 5; [238, 2026].

5.1.1 The Nature of Intelligence orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 5; [238, 2026].

5.1.2 The Nature of Intelligence conceptual primer: source context, core model, and reader task

This chapter teaches intelligence as a governed information cycle: requirements become collection, collection becomes evaluated evidence, evidence becomes analytic judgment, and judgment becomes a disseminated product with markings, records, feedback, and oversight. The chapter uses **Dissemination-and-Marking Control Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle**.
The central distinction is to separate intelligence work from ordinary research by naming authority, audience, caveats, and feedback. Core topics include **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle (Classic, Revised, and Critique); Types: Strategic, Operational, Tactical, Technical Intelligence**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Community, 2026]; [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026c]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [238, 2026]; [237, 2026].
Learners move from vocabulary and the **Dissemination-and-Marking Control Lens** distinction through topic lessons on **Defining Intelligence: Collection, Analysis, Production, Dissemination** with evidence and misconception checks, then assemble a **dissemination map with audience, caveat, marking, records, and feedback fields** with safety and rights gates.

5.1.3 The Nature of Intelligence learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 5; [238, 2026].

- Connect **Defining Intelligence: Collection, Analysis, Production, Dissemination and The Intelligence Cycle (Classic, Revised, and Critique)** to **Governed Intelligence Cycle and Dissemination Architecture** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **dissemination map with audience, caveat, marking, records, and feedback fields** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate intelligence work from ordinary research by naming authority, audience, caveats, and feedback; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as cycle theater, undocumented dissemination, classification drift, unclear release authority, stale records assumptions, and feedback loops that hide bias, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: cycle and marking material remains public-source and educational; it never handles classified content, live release decisions, or source-method exposure.

5.1.4 The Nature of Intelligence core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 5; [238, 2026].

Term	Working definition
Requirement	the decision need or learning question that justifies evidence collection
Dissemination	the controlled movement of an intelligence product to an authorized audience
Marking	the vocabulary that communicates handling, caveat, and release limits
Feedback loop	the customer or reviewer signal that tests whether the product answered the need
Records duty	the retention, deletion, or refresh obligation attached to an artifact
Decision hygiene	habits that keep requirements, evidence, and reviewer judgment aligned under load
Information architecture	how sources, notes, and products are organized so uncertainty stays visible
Defining Intelligence: Collection, Analysis,...	Key terms: Defining, Collection, Analysis.
The Intelligence Cycle (Classic, Revised, and...	Key terms: Cycle, Classic, Revised.

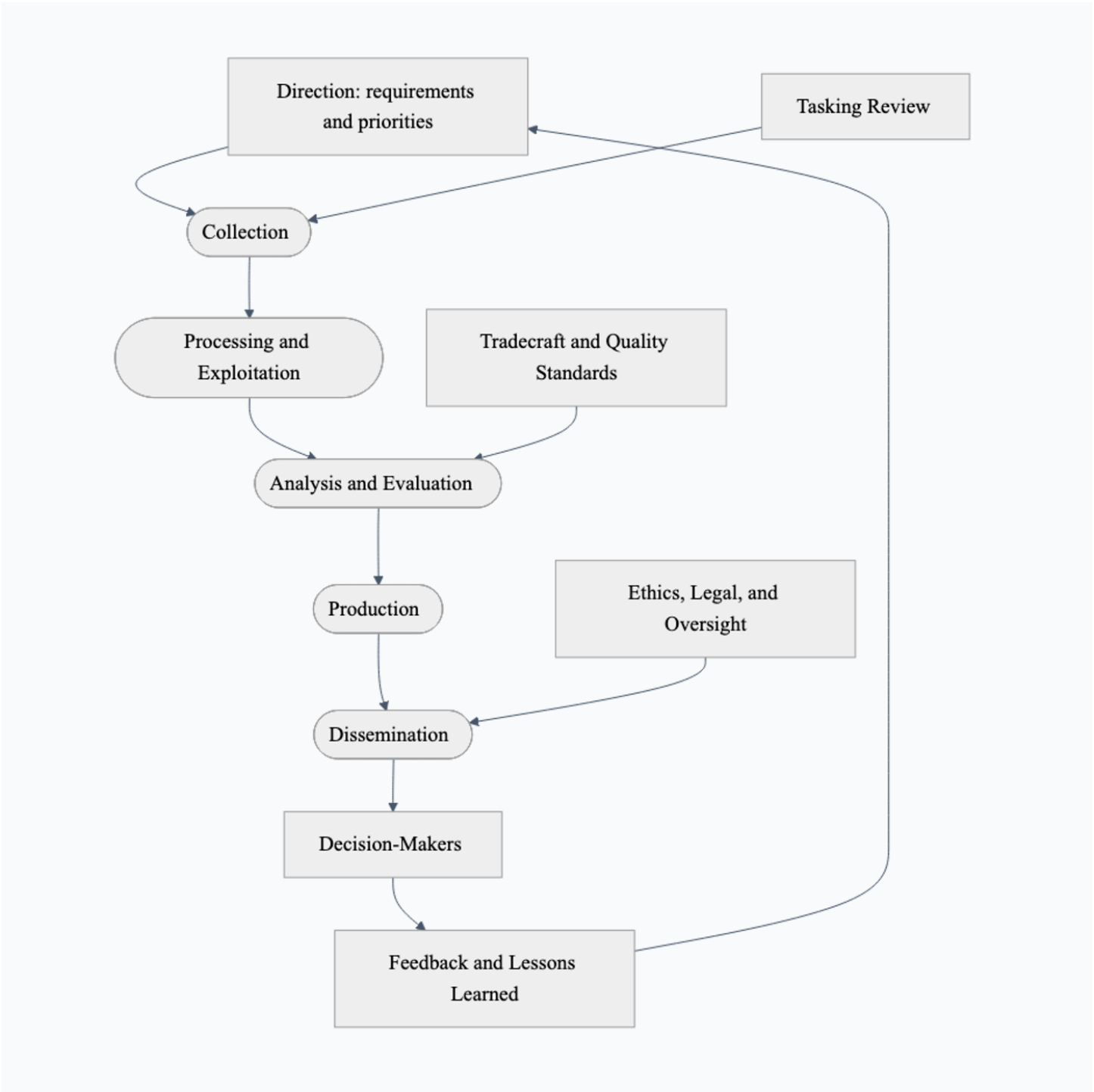


Figure 33: This diagram teaches the classic intelligence cycle as a governed, feedback-driven loop where each phase passes through review before products reach decision-makers. Its reader value is to make Direction: requirements and priorities, Decision-Makers, Feedback and Lessons Learned, and Tasking Review visible at a glance, with the foundations of intelligence tradecraft / the nature of intelligence section as the source section and defensive review as the boundary.

5.2 Dissemination-and-Marking Control Lens path for The Nature of Intelligence: lesson cluster, safe artifact, and review

Evidence anchor. Section 5; [238, 2026].

5.2.1 The Nature of Intelligence practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 5; [238, 2026].

5.2.2 The Nature of Intelligence topic lessons: source-backed concepts and transfer tasks

This module builds intelligence as a governed information cycle: requirements become collection, collection becomes evaluated evidence, evidence becomes analytic judgment, and judgment becomes a disseminated product with markings, records, feedback, and oversight. The sequence opens with **Defining Intelligence: Collection, Analysis, Production, Dissemination**, **The Intelligence Cycle (Classic, Revised, and Critique)**, **Types: Strategic, Operational, Tactical, Technical Intelligence** and applies the **Dissemination-and-Marking Control Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 30; module overview Section 5; curriculum atlas Section 2.

Triangulation anchors. In module 1's topic-lessons section, directly verified anchors for the **Governed Intelligence Cycle and Dissemination Architecture** lane include [Community, 2026]; [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026c]; [of the Director of National Intelligence, 2025a]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

5.2.2.1 Lesson 1: Defining Intelligence: Collection, Analysis, Production, Dissemination Concept. Defining Intelligence: Collection, Analysis, Production, Dissemination applies structured analytic methods with explicit alternatives, evidence tables, and calibrated confidence—not rhetorical certainty.

Why it matters. Analysts use **Defining Intelligence** to separate intelligence work from ordinary research by naming authority, audience, caveats, and feedback. A defensible treatment names the judgment it enables for cycle mapping and audience-aware product design review, the proof limit that collapsing reporting, inference, and judgment into one line would otherwise hide, and the reviewer accountable for challenge.

Source support. Defining Intelligence: Collection, Analysis, Production, Dissemination rests on [309, 2026], [310, 2026], and [300, 2026]. The lead source's own note reads: The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. Use them for the working definition that **Defining Intelligence: Collection, Analysis, Production, Dissemination** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2015].

Evidence to inspect. For **Defining Intelligence**, work from the cited evidence behind this row. [309, 2026] An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection. [310, 2026] The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Defining Intelligence**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this cycle mapping and audience-aware product design topic. The artifact must separate the source descriptor, the bounded judgment about **Defining Intelligence**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape **Defining Intelligence** work as a **requirements-to-product traceability ledger** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Defining Intelligence**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. Reuse the **Defining Intelligence** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

5.2.2.2 Lesson 2: The Intelligence Cycle (Classic, Revised, and Critique) Concept. The Intelligence Cycle (Classic, Revised, and Critique) traces requirements through collection, processing, analysis, dissemination, and feedback while naming authority and audience at each transition.

Why it matters. Without explicit treatment of **The Intelligence Cycle (Classic, Revised, and Critique)**, collapsing reporting, inference, and judgment into one line undermines cycle mapping and audience-aware product design review; the lesson builds the habit to separate intelligence work from ordinary research by naming authority, audience, caveats, and feedback.

Source support. The Intelligence Cycle (Classic, Revised, and Critique) rests on [297, 2026] and [298, 2026]. The closest source to this row notes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for the claim that **The Intelligence Cycle (Classic, Revised, and Critique)** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2015].

Evidence to inspect. For **The Intelligence Cycle (Classic, Revised, and Critique)**, reason from the sources cited in this row. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **The Intelligence Cycle (Classic, Revised, and Critique)**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this cycle mapping and audience-aware product design topic. The artifact must separate the source descriptor, the bounded judgment about **Intelligence Cycle**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape this subject work as a **requirements-to-product traceability ledger** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **The Intelligence Cycle (Classic, Revised, and Critique)**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. Transfer **The Intelligence Cycle (Classic, Revised, and Critique)** from this module to a second motif by preserving cycle mapping and audience-aware product design, replacing action with audit, and naming the blocked use.

5.2.2.3 Lesson 3: Types: Strategic, Operational, Tactical, Technical Intelligence Concept. Types: Strategic, Operational, Tactical, Technical Intelligence applies structured analytic methods with explicit alternatives, evidence tables, and calibrated confidence—not rhetorical

certainty.

Why it matters. Analysts use **Types: Strategic, Operational, Tactical, Technical Intelligence** to separate intelligence work from ordinary research by naming authority, audience, caveats, and feedback. A defensible treatment names the judgment it enables for cycle mapping and audience-aware product design review, the proof limit that collapsing reporting, inference, and judgment into one line would otherwise hide, and the reviewer accountable for challenge.

Source support. Types: Strategic, Operational, Tactical, Technical Intelligence rests on [309, 2026], [310, 2026], and [300, 2026]. The lead source's own note reads: It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). Use them for the working definition that **Types: Strategic, Operational, Tactical, Technical Intelligence** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2015].

Evidence to inspect. For **Types: Strategic, Operational, Tactical, Technical Intelligence**, work from the cited evidence behind this row. [309, 2026] An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection. [310, 2026] The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Types**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this cycle mapping and audience-aware product design topic. The artifact must separate the source descriptor, the bounded judgment about **Types**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape **Types: Strategic, Operational, Tactical, Technical Intelligence** work as a **requirements-to-product traceability ledger** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Types: Strategic, Operational, Tactical, Technical Intelligence**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. Transfer **Types: Strategic, Operational, Tactical, Technical Intelligence** from this module to a second motif by preserving cycle mapping and audience-aware product design, replacing action with audit, and naming the blocked use.

5.2.2.4 Lesson 4: Intelligence as Social and Epistemological Practice

Concept. Intelligence as Social and Epistemological Practice applies structured analytic methods with explicit alternatives, evidence tables, and calibrated confidence—not rhetorical certainty.

Why it matters. Without explicit treatment of **Intelligence as Social and Epistemological Practice**, collapsing reporting, inference, and judgment into one line undermines cycle mapping and audience-aware product design review; the lesson builds the habit to separate intelligence work from ordinary research by naming authority, audience, caveats, and feedback.

Source support. Intelligence as Social and Epistemological Practice uses curated analytic-tradecraft anchors [of the Director of National Intelligence, 2015]; [Agency, 2009]; [for the Study of Intelligence, 2002]; [Cooper, 2005]; [Johnston, 2005]; [on Terrorist Attacks Upon the United States, 2004]; [on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005]; [on Intelligence, 2004]; [Bruce, 2016]; [Coulthart, 2017]; [Tetlock, 2018]; [et al., 2019]; [Whitesmith, 2019]; [Mandel, 2020]; [Mandel, 2024]; [Barnes and Mandel, 2014]; [Tetlock, 2015b]; [Activity, 2010]; [Activity, 2023]; [McMahon, 2024]. The inherited guide citation(s) [001, 2026] remain context only; primary support must keep likelihood, confidence, assumptions, alternatives, dissent, source quality, ACH limits, and refresh duty separate. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2015].

Evidence to inspect. For **Intelligence as Social and Epistemological Practice**, use the curated analytic-tradecraft anchors [of the Director of National Intelligence, 2015]; [Agency, 2009]; [for the Study of Intelligence, 2002]; [Cooper, 2005]; [Johnston, 2005]; [on Terrorist Attacks Upon the United States, 2004]; [on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005]; [on Intelligence, 2004]; [Bruce, 2016]; [Coulthart, 2017]; [Tetlock, 2018]; [et al., 2019]; [Whitesmith, 2019]; [Mandel, 2020]; [Mandel, 2024]; [Barnes and Mandel, 2014]; [Tetlock, 2015b]; [Activity, 2010]; [Activity, 2023]; [McMahon, 2024]. Pull observation, inference, assumption, likelihood, confidence, dissent, decision-uptake boundary, postmortem learning, and the empirical limit that would force a weaker claim. Treat SATs as reviewable reasoning artifacts, not validated universal debiasing or autonomous judgment replacements.

Student artifact. For **Intelligence as Social and Epistemological Practice**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this cycle mapping and audience-aware product design topic. The artifact must separate the source descriptor, the bounded judgment about **Intelligence as Social and Epistemological**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape the same topic work as a **requirements-to-product traceability ledger** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Intelligence as Social and Epistemological Practice**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. Apply this module's safe boundary for **Intelligence as Social and Epistemological Practice** to another artifact while keeping cycle mapping and audience-aware product design and reviewer ownership explicit.

5.2.2.5 Lesson 5: National, Corporate, and Private Intelligence: Structural Differences

Concept. National, Corporate, and Private Intelligence: Structural Differences applies structured analytic methods with explicit alternatives, evidence tables, and calibrated confidence—not rhetorical certainty.

Why it matters. Analysts use **National, Corporate, and Private Intelligence** to separate intelligence work from ordinary research by naming authority, audience, caveats, and feedback. A defensible treatment names the judgment it enables for cycle mapping and audience-aware product design review, the proof limit that collapsing reporting, inference, and judgment into one line would otherwise hide, and the reviewer accountable for challenge.

Source support. National, Corporate, and Private Intelligence: Structural Differences rests on [297, 2026] and [298, 2026]. The lead source's own note reads: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for fixing what **National, Corporate, and Private Intelligence: Structural Differences** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2015].

Evidence to inspect. Ground **National, Corporate, and Private Intelligence** in the evidence the row cites. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **National, Corporate, and Private Intelligence**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this cycle mapping and audience-aware product design topic. The artifact must separate the source descriptor, the bounded judgment about **National Corporate and Private Intelligence**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape **National, Corporate, and Private Intelligence** work as a **requirements-to-product traceability**

ledger that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **National, Corporate, and Private Intelligence**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. Transfer **National, Corporate, and Private Intelligence** from this module to a second motif by preserving cycle mapping and audience-aware product design, replacing action with audit, and naming the blocked use.

5.2.2.6 Lesson 6: The Ethics of Intelligence: EO 12333, FISA, ICD 203, Allied Law

Concept. The Ethics of Intelligence: EO 12333, FISA, ICD 203, Allied Law — Calibrate confidence to evidence strength, source quality, and alternative explanations—not to rhetorical certainty.

Why it matters. Without explicit treatment of **The Ethics of Intelligence**, collapsing reporting, inference, and judgment into one line undermines cycle mapping and audience-aware product design review; the lesson builds the habit to separate intelligence work from ordinary research by naming authority, audience, caveats, and feedback.

Source support. The Ethics of Intelligence: EO 12333, FISA, ICD 203, Allied Law rests on [002, 2026]. Its anchor reference records: ICD 203 directs the heads of IC elements to designate a similar individual or office to respond. Use it for the working definition that **The Ethics of Intelligence: EO 12333, FISA, ICD 203, Allied Law** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2015].

Evidence to inspect. For **The Ethics of Intelligence**, reason from the sources cited in this row. [002, 2026] ICD 203 directs the heads of IC elements to designate a similar individual or office to respond. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **The Ethics of Intelligence**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this cycle mapping and audience-aware product design topic. The artifact must separate the source descriptor, the bounded judgment about **Ethics of Intelligence**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape **The Ethics of Intelligence** work as a **requirements-to-product traceability ledger** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **The Ethics of Intelligence**: that a legal source grants authority without scope and oversight.

Transfer task. Transfer **The Ethics of Intelligence** from this module to a second motif by preserving cycle mapping and audience-aware product design, replacing action with audit, and naming the blocked use.

5.2.2.7 Lesson 7: Active Inference as a Unifying Cognitive Framework for Intelligence

Concept. Active Inference as a Unifying Cognitive Framework for Intelligence treats active inference as an agent-modeling vocabulary: beliefs, actions, expected observations, and policy selection are classroom concepts, not proof that an intelligence agent should act autonomously.

Why it matters. Active Inference connects classroom vocabulary to Governed Intelligence Cycle and Dissemination Architecture practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Active Inference as a Unifying Cognitive Framework for Intelligence rests on [003, 2026]. The lead source's own note reads: It maps concepts such as variational free energy, prediction error, generative models, and Markov blankets onto industrial engineering and quality management practices, treating organizational survival as the maintenance of process control limits. Use it for pinning down the scope of **Active Inference as a Unifying Cognitive Framework for Intelligence**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2015].

Evidence to inspect. Read **Active Inference** against the works cited for this row. [003, 2026] A 2021 peer-reviewed article by Stephen Fox in the journal Entropy that relates the active inference framework to social organization. It maps concepts such as variational free energy, prediction error, generative models, and Markov blankets onto industrial engineering and quality management practices, treating organizational survival as the maintenance of process control limits. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Active Inference**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this cycle mapping and audience-aware product design topic. The artifact must separate the source descriptor, the bounded judgment about **Active Inference as a Unifying**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape **Active Inference** work as a **requirements-to-product traceability ledger** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Active Inference**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. For **Active Inference**, transfer the idea to a non-AI chapter by naming the assumed model, the surprising observation, and the review point before any decision follows.

5.2.2.8 Lesson 8: The AI Inflection Point: How Artificial Intelligence Reshapes Every Phase of the Intelligence Cycle

Concept. The AI Inflection Point: How Artificial Intelligence Reshapes Every Phase of the Intelligence Cycle traces requirements through collection, processing, analysis, dissemination, and feedback while naming authority and audience at each transition.

Why it matters. Without explicit treatment of **The AI Inflection Point**, collapsing reporting, inference, and judgment into one line undermines cycle mapping and audience-aware product design review; the lesson builds the habit to separate intelligence work from ordinary research by naming authority, audience, caveats, and feedback.

Source support. The AI Inflection Point: How Artificial Intelligence Reshapes Every Phase of the Intelligence Cycle rests on [004, 2026] and [005, 2026]. Its anchor reference records: 1, March 2026). Use them for fixing what **The AI Inflection Point: How Artificial Intelligence Reshapes Every Phase of the Intelligence Cycle** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2015].

Evidence to inspect. For **The AI Inflection Point**, reason from the sources cited in this row. [004, 2026] Tom Mulligan argues that artificial intelligence will enhance rather than replace human intelligence professionals, contending that the future of intelligence lies in human-machine collaboration. He maintains that uniquely human qualities such as intuition, experience, and independent judgment become more valuable as adversaries gain access to the same AI tools. [005, 2026] A blog post on SemperVerus summarizing a CIA Studies in Intelligence article, "Espionage in Our AI Future: Why Human Intelligence Still Matters" (Vol. 70, No. 1, March 2026). It argues that as AI makes technical intelligence cheaper and AI-driven fabrication more pervasive, human intelligence becomes relatively more valuable, since human specialists are needed to verify source reliability over time. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **The AI Inflection Point**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this cycle mapping and audience-aware product design topic. The artifact must separate the source descriptor, the bounded judgment about **AI Inflection Point**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape **The AI Inflection Point** work as a **requirements-to-product traceability ledger** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **The AI Inflection Point**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. Transfer **The AI Inflection Point** from this module to a second motif by preserving cycle mapping and audience-aware product design, replacing action with audit, and naming the blocked use.

5.2.3 The Nature of Intelligence worked safe example: synthetic inputs, evidence, and review

Worked example: a synthetic analyst team rebuilds a storm-impact brief after discovering a stale requirement and overloaded reading queue. [238, 2026]; [237, 2026].

Triangulation anchors. In module 1's worked-example section, directly verified anchors for the **Governed Intelligence Cycle and Dissemination Architecture** lane include [Community, 2026]; [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026c]; [of the Director of National Intelligence, 2025a]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **intelligence-cycle governance**. Learners use a **requirements-to-product traceability ledger** and keep this boundary visible: Activities stay inside public, synthetic, or instructor-provided materials and never become live collection or tasking.

Frame. The classroom question centers on **Defining Intelligence: Collection, Analysis, Production, Dissemination**. Excluded actions stay explicit, and the **Dissemination-and-Marking Control Lens** planning question is: Which audience, release authority, marking vocabulary, records duty, and feedback loop governs this intelligence artifact?

Inputs. For the **Defining Intelligence: Collection, Analysis, Production, Dissemination** scenario, use public weather bulletins, public infrastructure maps, historical outage summaries, and instructor-provided toy records. The Dissemination-and-Marking Control Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Defining Intelligence: Collection, Analysis, Production, Dissemination**, students map the requirement, tag each source, separate observation from judgment, assign caveats, and record the dissemination audience. Pause whenever an inference about Defining Intelligence: Collection, Analysis, Production, Dissemination appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Defining Intelligence: Collection, Analysis, Production, Dissemination** classroom scenario; unit artifact = requirements-to-product traceability ledger; evidence = allowed inputs; method = cycle mapping and audience-aware product design; output = a one-page release-neutral brief with source descriptors, confidence language, caveats, and a feedback owner; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Defining Intelligence: Collection, Analysis, Production, Dissemination** as "Dissemination-and-Marking Control Lens confirms it" is not enough. The revision ties the claim to cycle mapping and audience-aware product design, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Defining Intelligence: Collection, Analysis, Production, Dissemination** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

5.2.4 The Nature of Intelligence practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Dissemination-and-Marking Control Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle**.

Triangulation anchors. In module 1's practice-sequence section, directly verified anchors for the **Governed Intelligence Cycle and Dissemination Architecture** lane include [Community, 2026]; [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026c]; [of the Director of National Intelligence, 2025a]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Defining Intelligence: Collection, Analysis, Production, Dissemination, The Intelligence Cycle, Types: Strategic, Operational, Tactical, Technical Intelligence; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Governed Intelligence Cycle and Dissemination Architecture** lane.
2. Frame	Answer the lens question: Which audience, release authority, marking vocabulary, records duty, and feedback loop governs this intelligence artifact?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Defining Intelligence: Collection, Analysis, Production, Dissemination: dissemination map with audience, caveat, marking, records, and feedback fields.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the requirements-to-product traceability ledger fields for Defining Intelligence: Collection, Analysis, Production, Dissemination.	Unit profile note.	Evidence artifacts include requirement card, source descriptor.
4. Challenge	Test the misconception that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.	Failure-mode note.	The artifact applies the key distinction: separate intelligence work from ordinary research by naming authority, audience, caveats, and feedback.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

5.2.4.1 The Nature of Intelligence instructor notes: source reasoning, review points, and studio focus

Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human

review point. Keep the focus on **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle**. [238, 2026]; [237, 2026].

5.2.4.2 The Nature of Intelligence extension exercise: peer validation and refresh trigger review **Evidence anchor.** Section 5; [238, 2026].
Have learners swap artifacts and apply the **Dissemination-and-Marking Control Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle**.

5.2.5 The Nature of Intelligence knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 5; [238, 2026].

1. Explain how **Defining Intelligence: Collection, Analysis, Production, Dissemination** is defined here; name the source descriptor that supports the definition.
2. Contrast **Defining Intelligence: Collection, Analysis, Production, Dissemination** with **The Intelligence Cycle** using the **Dissemination-and-Marking Control Lens** artifact fields.
3. Identify one failure mode from the **Governed Intelligence Cycle and Dissemination Architecture** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which requirement, source, or workflow step failed first when the team ran out of review time?
5. Correct this misconception: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

5.2.5.1 The Nature of Intelligence answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Defining Intelligence: Collection, Analysis, Production, Dissemination** without source evidence, uncertainty, or a safe transfer task.

5.3 The Nature of Intelligence assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 5; [238, 2026].

5.3.1 The Nature of Intelligence evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 5; [238, 2026].

5.3.2 The Nature of Intelligence transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 5; [238, 2026].

5.3.2.1 The Nature of Intelligence lineage and source tradition: profile, concepts, and first anchors This sits in the **Governed Intelligence Cycle and Dissemination Architecture** lineage: treating the intelligence cycle as a governed information system whose collection, processing, analysis, dissemination, evaluation, marking, and records obligations stay explicit. [238, 2026]; [237, 2026].

5.3.2.2 The Nature of Intelligence working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 5; [238, 2026].
The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle**, with provenance and reviewability throughout.

5.3.2.3 The Nature of Intelligence knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** requirements, audience needs, public-source evidence, caveats, and feedback signals. [238, 2026]; [237, 2026].
- **Transforms:** requirement framing, collection scoping, source evaluation, analytic judgment, dissemination, and feedback review.
- **Outputs:** release-neutral brief, audience map, caveat register, and feedback note.
- **Failure modes:** unscoped audiences, missing caveats, weak records, and product reuse without feedback.

5.3.2.4 The Nature of Intelligence transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 5; [238, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle**.
- **Evidence contract:** keep the **Governed Intelligence Cycle and Dissemination Architecture** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as release-neutral brief, audience map, caveat register, and feedback note that another reviewer can audit.

5.3.2.5 The Nature of Intelligence profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 5; [238, 2026].
The matched profile emphasizes treating the intelligence cycle as a governed information system whose collection, processing, analysis, dissemination, evaluation, marking, and records obligations stay explicit. The method stack is cycle mapping, priority-to-product traceability, data-lifecycle mapping, classification vocabulary review, dissemination-caveat audit, customer feedback, and oversight checkpointing; the local topic cluster is **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle**.

5.3.3 The Nature of Intelligence evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 5; [238, 2026].
Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Governed Intelligence Cycle and Dissemination Architecture** profile tells reviewers what evidence is strong enough for the module artifact built around **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle**.

5.3.3.1 The Nature of Intelligence guide source spine: inherited keys and local citation roles Primary guide citations: [238, 2026]; [237, 2026]; [270, 2026]; [273, 2026]; [274, 2026]; [275, 2026]; [286, 2026]; [287, 2026]; [292, 2026]; [001, 2026]; [002, 2026]; [003, 2026]; [004, 2026]; [005, 2026]; [297, 2026]; [298, 2026]; [309, 2026]; [310, 2026]; [300, 2026].

5.3.3.2 The Nature of Intelligence verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [238, 2026]; [237, 2026].

Tier	What counts	How it is used
Source guide	[238, 2026]; [237, 2026]; [270, 2026]; [273, 2026]; [274, 2026]; [275, 2026]; [286, 2026]; [287, 2026]; [292, 2026]; [001, 2026]; [002, 2026]; [003, 2026]; [004, 2026]; [005, 2026]; [297, 2026]; [298, 2026]; [309, 2026]; [310, 2026]; [300, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 1's source-canon section, directly verified anchors for the **Governed Intelligence Cycle and Dissemination Architecture** lane include [Community, 2026]; [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026c]; [of the Director of National Intelligence, 2025a]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Maintenance rule: Perplexity may suggest candidates for **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle** and [238, 2026]; [237, 2026], but only directly verified source URLs are encoded as citations.

5.3.3.3 The Nature of Intelligence intelligence practice lens: evidence artifact and safety check Practice lens: **Dissemination-and-Marking Control Lens** for **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle**. [238, 2026]; [237, 2026].

Planning question: Which audience, release authority, marking vocabulary, records duty, and feedback loop governs this intelligence artifact?

Evidence artifact: dissemination map with audience, caveat, marking, records, and feedback fields.

Validation rule: verify source authority, public/classification status, CAPCO-safe vocabulary, audience need, and records disposition before reuse. Applied to **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle**.

Handoff contract: deliver release-neutral summaries, source metadata, marking rationale, and review ownership as separate fields.

Safety check: exclude classified content, live release decisions, source-method exposure, and improvised control markings.

5.3.3.4 The Nature of Intelligence runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 5; [238, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	1.99	1.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind The Nature of Intelligence to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Bounded autonomy, procurement, incident-response, and assurance studio	1.101	1.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for The Nature of Intelligence	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Model-card, recoverability, retention, and learner-support evidence package	1.102	1.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for The Nature of Intelligence	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Defining Intelligence: Collection, Analysis, Production, Dissemination	1.1	1.1 Defining Intelligence: Collection, Analysis, Production, Dissemination	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
The Intelligence Cycle (Classic, Revised, and Critique)	1.2	1.2 The Intelligence Cycle (Classic, Revised, and Critique)	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Types: Strategic, Operational, Tactical, Technical Intelligence	1.3	1.3 Types: Strategic, Operational, Tactical, Technical Intelligence	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Intelligence as Social and Epistemological Practice	1.4	1.4 Intelligence as Social and Epistemological Practice	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
National, Corporate, and Private Intelligence: Structural Differences	1.5	1.5 National, Corporate, and Private Intelligence: Structural Differences	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
The Ethics of Intelligence: EO 12333, FISA, ICD 203, Allied Law	1.6	1.6 The Ethics of Intelligence: EO 12333, FISA, ICD 203, Allied Law	AI/Data Accountability Lens	AI/data impact card with authority, provenance, model version, impact score, register status, human owner, and review cadence	reject automated adverse action, hidden surveillance expansion, unowned outputs, unreviewed model drift, and opaque downstream reuse
Active Inference as a Unifying Cognitive Framework for Intelligence	1.7	1.7 Active Inference as a Unifying Cognitive Framework for Intelligence	Active-Inference Boundary Lens	theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition	reject claims that the free-energy principle proves autonomous agency, intent, detection performance, or oversight-free action
The AI Inflection Point: How Artificial Intelligence Reshapes Every Phase of the Intelligence Cycle	1.8	1.8 The AI Inflection Point: How Artificial Intelligence Reshapes Every Phase of the Intelligence Cycle	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence

5.3.3.5 The Nature of Intelligence reusable subsection contract: topic rows, artifacts, and safety duties **Evidence anchor.** Section 5; [238, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Defining Intelligence: Collection, Analysis, Production, Dissemination	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
The Intelligence Cycle (Classic, Revised, and Critique)	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Types: Strategic, Operational, Tactical, Technical Intelligence	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Intelligence as Social and Epistemological Practice	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
National, Corporate, and Private Intelligence: Structural Differences	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
The Ethics of Intelligence: EO 12333, FISA, ICD 203, Allied Law	AI/Data Accountability Lens	AI/data impact card with authority, provenance, model version, impact score, register status, human owner, and review cadence	reject automated adverse action, hidden surveillance expansion, unowned outputs, unreviewed model drift, and opaque downstream reuse
Active Inference as a Unifying Cognitive Framework for Intelligence	Active-Inference Boundary Lens	theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition	reject claims that the free-energy principle proves autonomous agency, intent, detection performance, or oversight-free action
The AI Inflection Point: How Artificial Intelligence Reshapes Every Phase of the Intelligence Cycle	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence

5.3.3.6 The Nature of Intelligence annotated source ledger: real titles and local contribution Each source cited by this **Governed Intelligence Cycle and Dissemination Architecture** module is paired below with its real title and a one-line note on what it contributes to **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle**.

Source	Cited work	What it contributes	Status
[238, 2026]	Recommendation on the Ethics of Artificial Intelligence	The official UNESCO page for the Recommendation on the Ethics of Artificial Intelligence, the first global standard-setting instrument on AI ethics, adopted in 2021 and applicable to all 194 member states. It outlines four core values, including human rights protection and environmental flourishing, and ten guiding principles such as proportionality, privacy, transparency, and fairness.	verified source-guide
[237, 2026]	Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities	Official GAO AI accountability framework.	original source-guide
[270, 2026]	NIST Big Data Interoperability Framework	NIST Special Publication 1500-1 (revised edition by Chang and Grady) establishes foundational terminology and consensus definitions for Big Data through the NIST Big Data Public Working Group. The volume defines Big Data characteristics, taxonomy, and a reference architecture assigning roles to Application Providers, Data Consumers, Data Providers, and System Orchestrators.	verified source-guide
[273, 2026]	WCAG 2 Overview	The W3C Web Accessibility Initiative overview of the Web Content Accessibility Guidelines (WCAG), an international standard for making web content accessible to people with disabilities. It explains that WCAG is organized around four principles (perceivable, operable, understandable, robust) with testable success criteria at three conformance levels (A, AA, AAA), and covers versions 2.0, 2.1, and 2.2.	verified source-guide
[274, 2026]	CAST Universal Design for Learning Guidelines version 3.0	The official CAST website for the Universal Design for Learning (UDL) Guidelines version 3.0, released in 2024. The framework offers research-based guidance for designing inclusive learning environments and is organized around three principles: Engagement (motivation and emotional support), Representation (accessible presentation of information), and Action and Expression (diverse means of participation and communication).	verified source-guide
[275, 2026]	Fact Sheet: New Rule on the Accessibility of Web Content and Mobile Apps Provided by State and Local Governments	A US Department of Justice fact sheet explaining the 2024 ADA Title II rule requiring state and local governments to make their web content and mobile apps accessible. It establishes WCAG 2.1 Level AA as the technical standard, applies to entities such as schools, courts, libraries, and transit agencies, and sets compliance deadlines of April 2027 for larger jurisdictions and April 2028 for smaller ones.	verified source-guide

Source	Cited work	What it contributes	Status
[286, 2026]	Model Cards for Model Reporting	The arXiv abstract for "Model Cards for Model Reporting" (2018) by Mitchell, Wu, Zaldivar, and colleagues, which introduces a framework for transparent documentation of machine learning models. Model cards are short accompanying documents that report a model's benchmarked performance across varied conditions, including different cultural, demographic, and phenotypic groups, along with intended use, evaluation methodology, and deployment considerations.	verified source-guide
[287, 2026]	Datasheets for Datasets	A 2018 arXiv paper proposing 'datasheets for datasets,' a standardized documentation framework for machine learning datasets modeled on electronic component datasheets. The authors argue the field lacks consistent dataset documentation, which creates risk in high-stakes applications, and propose that datasets be accompanied by documentation covering motivation, composition, collection process, recommended uses, and test results.	verified source-guide
[292, 2026]	Assessing Risks and Impacts of AI (ARIA): Pilot Evaluation Report	The ARIA 0.1 pilot evaluation report documents NIST's methodology for systematically assessing AI applications for risks and societal impacts, using a multi-layered evaluation approach across five participating organizations and seven submitted AI applications. The pilot employed three evaluation scenarios and three testing levels: model testing, red teaming, and field testing, supplemented by dialogue annotation, tester questionnaires, and structured measurement trees.	verified source-guide
[001, 2026]	Epistemic Governance in the Context of Crisis	This article examines the concept of epistemic governance during crises.	original source-guide
[002, 2026]	Objectivity	ICD 203 directs the heads of IC elements to designate a similar individual or office to respond.	original source-guide
[003, 2026]	Active Inference: Applicability to Different Types of Social	A 2021 peer-reviewed article by Stephen Fox in the journal Entropy that relates the active inference framework to social organization. It maps concepts such as variational free energy, prediction error, generative models, and Markov blankets onto industrial engineering and quality management practices, treating organizational survival as the maintenance of process control limits.	verified source-guide
[004, 2026]	AI Won't Replace Spies—It Will Make Them More Powerful Than Ever	Tom Mulligan argues that artificial intelligence will enhance rather than replace human intelligence professionals, contending that the future of intelligence lies in human-machine collaboration. He maintains that uniquely human qualities such as intuition, experience, and independent judgment become more valuable as adversaries gain access to the same AI tools.	verified source-guide

Source	Cited work	What it contributes	Status
[005, 2026]	CIA: Studies in AI and Human Intelligence - SemperVerus	A blog post on SemperVerus summarizing a CIA Studies in Intelligence article, "Espionage in Our AI Future: Why Human Intelligence Still Matters" (Vol. 70, No. 1, March 2026). It argues that as AI makes technical intelligence cheaper and AI-driven fabrication more pervasive, human intelligence becomes relatively more valuable, since human specialists are needed to verify source reliability over time.	verified source-guide
[297, 2026]	Intelligence Community Directive 203: Analytic Standards	Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products.	original source-guide
[298, 2026]	Intelligence Community Directives	Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations.	original source-guide
[309, 2026]	STIX Version 2.1	An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection.	verified source-guide
[310, 2026]	TAXII Version 2.1	The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe).	verified source-guide
[300, 2026]	MITRE ATLAS	MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy.	original source-guide

Where this sits. This module's overview is Section 5; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

5.3.4 The Nature of Intelligence governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 5; [238, 2026].

5.3.5 The Nature of Intelligence analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 1's governance-boundary section, directly verified anchors for the **Governed Intelligence Cycle and Dissemination Architecture** lane include [Community, 2026]; [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026c]; [of the Director of National Intelligence, 2025a]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **Governed Intelligence Cycle and Dissemination Architecture** for **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle (Classic, Revised, and Critique)**. [238, 2026]; [237, 2026].

Curriculum topic spine: Defining Intelligence: Collection, Analysis, Production, Dissemination, **The Intelligence Cycle (Classic, Revised, and Critique)**, **Types: Strategic, Operational, Tactical, Technical Intelligence**. **Verified anchor cluster:** [Community, 2026]; [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026c]; [of the Director of National Intelligence, 2025a]; [of the Director of National Intelligence, 2026b]; [General Services Administration et al., 2026]; [Privacy and Board, 2026].

Conceptual depth: treating the intelligence cycle as a governed information system whose collection, processing, analysis, dissemination, evaluation, marking, and records obligations stay explicit.

Method stack: cycle mapping, priority-to-product traceability, data-lifecycle mapping, classification vocabulary review, dissemination-caveat audit, customer feedback, and oversight checkpointing.

Composability contract: requirements, data provenance, analytic judgments, markings, dissemination permissions, records obligations, and feedback remain separable artifacts.

Known failure modes: cycle theater, undocumented dissemination, classification drift, unclear release authority, stale records assumptions, and feedback loops that hide bias.

Defensive boundary: cycle and marking material remains public-source and educational; it never handles classified content, live release decisions, or source-method exposure. Applied to **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle (Classic, Revised, and Critique)**.

Anchor	Why it matters here
[Community, 2026]	Official public explanation of the intelligence cycle, collection disciplines, dissemination, evaluation, oversight, and partners. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2015]	Official ODNI analytic tradecraft standards directive. Checked as of 2026-05-21; role: source_quality_anchor.
[of the Director of National Intelligence, 2026c]	Official prioritization directive for translating national intelligence priorities into collection, analysis, risk management, and responsiveness evaluation. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2025a]	Official IC data-management directive for data governance, data stewardship, CDO authority, interoperability, and data lifecycle management. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026b]	Official CAPCO register for classification and control-marking vocabulary, abbreviations, portion markings, and dissemination syntax. Checked as of 2026-05-21; role: curriculum_anchor.
[General Services Administration et al., 2026]	Official federal data-governance benchmark for data as a strategic asset, ethical governance, lifecycle practices, and learning culture. Checked as of 2026-05-21; role: curriculum_anchor.
[Privacy and Board, 2026]	Official oversight-report library for privacy, civil-liberties, surveillance, watchlisting, facial-recognition, and redress analysis. Checked as of 2026-05-21; role: curriculum_anchor.

5.3.5.1 The Nature of Intelligence evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **Governed Intelligence Cycle and Dissemination Architecture** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [238, 2026]; [237, 2026].

5.3.6 The Nature of Intelligence agentic boundary: assist, approve, block, and record

Evidence anchor. Section 5; [238, 2026].

AGEINT translation is bounded by the **Governed Intelligence Cycle and Dissemination Architecture** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle**.

5.3.6.1 The Nature of Intelligence permitted defensive utility: curriculum uses and safe outputs

Evidence anchor. Section 5; [238, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle**.

5.3.6.2 The Nature of Intelligence excluded operational boundary: blocked actions and stop rules

Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [238, 2026]; [237, 2026] and **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

5.3.7 The Nature of Intelligence governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 5; [238, 2026].

Governance is practiced as a gate on the **Governed Intelligence Cycle and Dissemination Architecture** lane. Learners use the **Dissemination-and-Marking Control Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when

an agent-assisted artifact must stop for human review while using **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle**.

5.3.7.1 The Nature of Intelligence governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [238, 2026]; [237, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Governed Intelligence Cycle and Dissemination Architecture** failure modes and the **Dissemination-and-Marking Control Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

5.3.7.2 The Nature of Intelligence evidence package handoff: appendices, records, and reuse **Evidence anchor.** Section 5; [238, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Dissemination-and-Marking Control Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle**.

5.3.7.3 The Nature of Intelligence current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle**. [238, 2026]; [237, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_intelligence_gov_how_ic_works` for **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle**?	How the IC Works; lane `governed_intelligence_cycle`; checked 2026-05-21.	dissemination map with audience, caveat, marking, records, and feedback fields; Official public explanation of the intelligence cycle, collection disciplines, dissemination, evaluation, oversight, and partners.
What does the module inherit from `official_odni_icd_203` for **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle**?	Intelligence Community Directive 203: Analytic Standards; lane `source_quality_spine`; checked 2026-05-21.	dissemination map with audience, caveat, marking, records, and feedback fields; Official ODNI analytic tradecraft standards directive.
What does the module inherit from `official_odni_icd_204` for **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle**?	Intelligence Community Directive 204: National Intelligence Priorities Framework; lane `collection_management`; checked 2026-05-21.	dissemination map with audience, caveat, marking, records, and feedback fields; Official prioritization directive for translating national intelligence priorities into collection, analysis, risk management, and responsiveness evaluation.
What does the module inherit from `official_odni_icd_504` for **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle**?	Intelligence Community Directive 504: Intelligence Community Data Management; lane `ai_ethics_data_governance`; checked 2026-05-21.	dissemination map with audience, caveat, marking, records, and feedback fields; Official IC data-management directive for data governance, data stewardship, CDO authority, interoperability, and data lifecycle management.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 5; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

5.3.8 The Nature of Intelligence assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 5; [238, 2026].

5.3.9 The Nature of Intelligence assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 5; [238, 2026].

5.3.9.1 The Nature of Intelligence capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle** and [238, 2026]; [237, 2026].

5.3.9.2 The Nature of Intelligence instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle** and [238, 2026]; [237, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

5.3.9.3 The Nature of Intelligence assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Defining Intelligence: Collection, Analysis, Production, Dissemination	Completed **dissemination map with audience, caveat, marking, records, and feedback fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
The Intelligence Cycle (Classic, Revised, and Critique)	Completed **dissemination map with audience, caveat, marking, records, and feedback fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Types: Strategic, Operational, Tactical, Technical Intelligence	Completed **dissemination map with audience, caveat, marking, records, and feedback fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

5.3.10 The Nature of Intelligence refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [238, 2026]; [237, 2026] and **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle**.

5.3.10.1 The Nature of Intelligence refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle**. The local signals begin with [238, 2026]; [237, 2026].

5.3.10.2 The Nature of Intelligence claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle**, and the source spine for these checks begins with [238, 2026]; [237, 2026].

5.3.11 The Nature of Intelligence reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [238, 2026]; [237, 2026].

Triangulation anchors. In module 1's review-checklist section, directly verified anchors for the **Governed Intelligence Cycle and Dissemination Architecture** lane include [Community, 2026]; [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026c]; [of the Director of National Intelligence, 2025a]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle**. [238, 2026]; [237, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

5.3.12 The Nature of Intelligence learning-path links: module map, overview, and curriculum atlas

Follow the cross-links to move between **Defining Intelligence: Collection, Analysis, Production, Dissemination; The Intelligence Cycle** and the rest of the curriculum without losing the source spine: orientation first, then the parent unit, then the modules on either side. Primary sources: [238, 2026]; [237, 2026].

Section 2, Section 4, Section 6

6 Intelligence Community Architectures

6.0.1 Intelligence Community Architectures figures and course links: visual evidence, source flow, and navigation

The module uses Figure 34 and Figure 30 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 4, Section 5, Section 7.
This module teaches the **Analytic Tradecraft and Source Integrity** lane through a bounded, source-backed coursebook chapter. [234, 2026]; [247, 2026].

6.1 Analytic Tradecraft and Source Integrity frame for Intelligence Community Architectures: source context, topic focus, and reader task

Evidence anchor. Section 6; [234, 2026].

6.1.1 Intelligence Community Architectures orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 6; [234, 2026].

6.1.2 Intelligence Community Architectures conceptual primer: source context, core model, and reader task

This chapter teaches analytic tradecraft as disciplined judgment under uncertainty: claims become useful only when evidence, assumptions, alternatives, confidence, and dissent remain visible. The chapter uses **Dissemination-and-Marking Control Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**.
The central distinction is to separate reporting from inference, and inference from judgment. Core topics include **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study; British Architecture: Declassified source-protection and institutional-control case study**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2026e]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [234, 2026]; [247, 2026].
Learners move from vocabulary and the **Dissemination-and-Marking Control Lens** distinction through topic lessons on **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships** with evidence and misconception checks, then assemble a **dissemination map with audience, caveat, marking, records, and feedback fields** with safety and rights gates.

6.1.3 Intelligence Community Architectures learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 6; [234, 2026].

- Connect **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships and Declassified source-protection and institutional-control case study** to **Analytic Tradecraft and Source Integrity** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **dissemination map with audience, caveat, marking, records, and feedback fields** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate reporting from inference, and inference from judgment; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as source laundering, automation bias, hidden assumptions, collapsed likelihood/confidence language, hindsight certainty, SAT-as-bias-cure overclaiming, and visually persuasive but weakly sourced claims, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: analysis remains educational and decision-supportive; it does not become tasking, targeting, covert collection, or policy advocacy.

6.1.4 Intelligence Community Architectures core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 6; [234, 2026].

Term	Working definition
Source descriptor	a compact statement of where evidence came from and what it can support
Assumption	a claim accepted for analysis that still needs challenge
Alternative hypothesis	a plausible explanation that competes with the favored account
Confidence	a calibrated expression of evidentiary strength and analytic uncertainty
Dissent	a documented disagreement that preserves minority reasoning for review
U.S. Intelligence Community: 18 Agencies,…	Key terms: Community, Agencies, Authorities.
Declassified source-protection and…	Key terms: Declassified, protection, institutional.

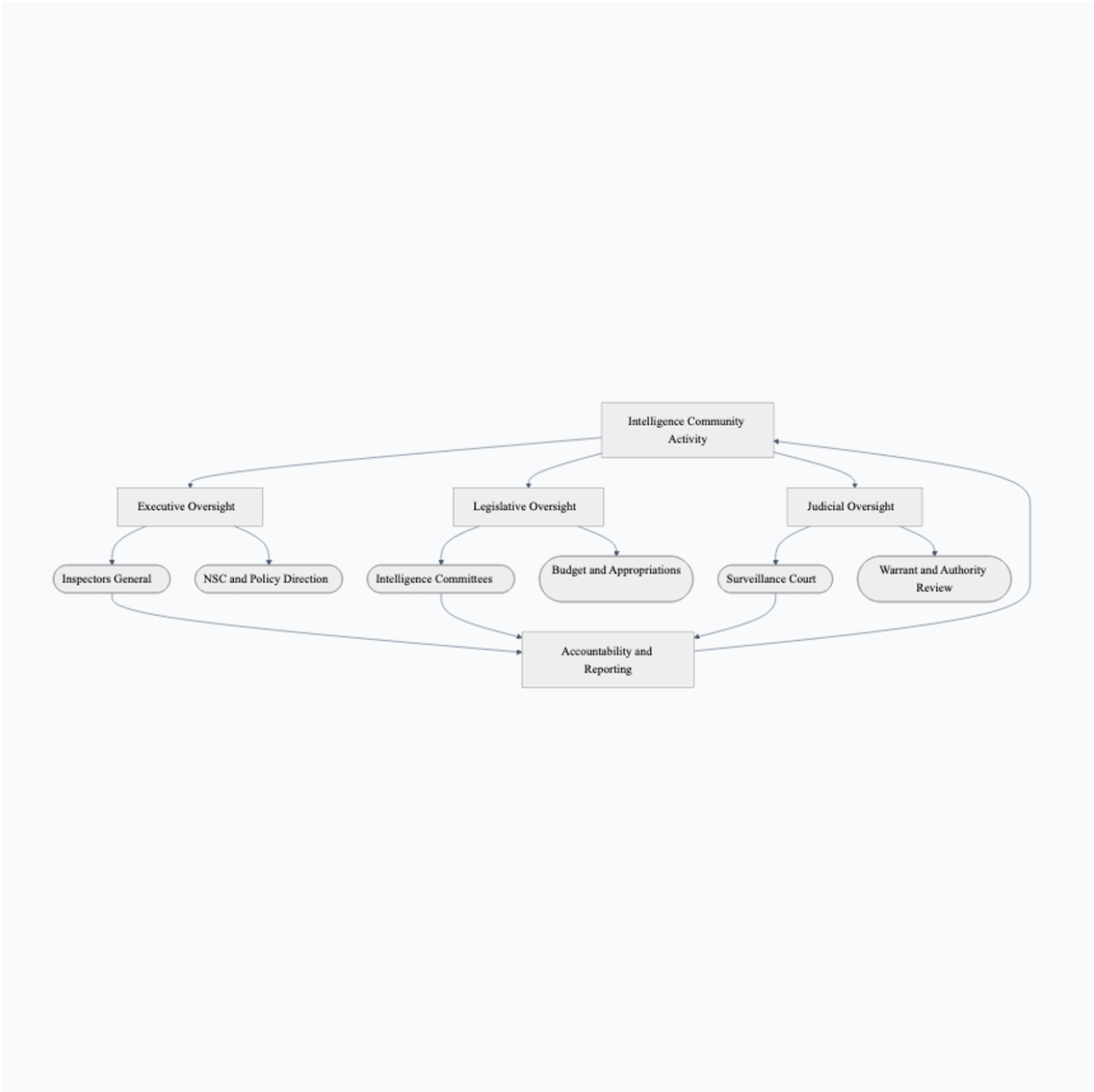


Figure 34: This diagram teaches how executive, legislative, and judicial oversight mechanisms jointly constrain and supervise intelligence community activity. It is anchored to the foundations of intelligence tradecraft / intelligence community architectures section; use it to inspect Intelligence Community Activity, Executive Oversight, Legislative Oversight, and Judicial Oversight while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

6.2 Dissemination-and-Marking Control Lens path for Intelligence Community Architectures: lesson cluster, safe artifact, and review

Evidence anchor. Section 6; [234, 2026].

6.2.1 Intelligence Community Architectures practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 6; [234, 2026].

6.2.2 Intelligence Community Architectures topic lessons: source-backed concepts and transfer tasks

This module builds analytic tradecraft as disciplined judgment under uncertainty: claims become useful only when evidence, assumptions, alternatives, confidence, and dissent remain visible. The sequence opens with **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships**, **Declassified source-protection and institutional-control case study**, **British Architecture: Declassified source-protection and institutional-control case study** and applies the **Dissemination-and-Marking Control Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 30; module overview Section 6; curriculum atlas Section 2.

Triangulation anchors. In module 2's topic-lessons section, directly verified anchors for the **Analytic Tradecraft and Source Integrity** lane include [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2026e]; [Agency, 2009]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

6.2.2.1 Lesson 1: U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships

Concept. U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships maps the theory to institutions: priorities, feedback, incentives, review loops, and records shape what an intelligence community notices and ignores.

Why it matters. Without explicit treatment of **U.S. Intelligence Community**, source laundering undermines structured reasoning and source-integrity review; the lesson builds the habit to separate reporting from inference, and inference from judgment.

Source support. U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships rests on [006, 2026]. The lead source's own note reads: ICDs are the principal means by which the DNI provides policy, guidance, and direction to the U.S. Use it for pinning down the scope of **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. For **U.S. Intelligence Community**, reason from the sources cited in this row. [006, 2026] A Federation of American Scientists repository cataloguing the Intelligence Community Directives (ICDs) issued by the Director of National Intelligence. ICDs are the principal means by which the DNI provides policy, guidance, and direction to the U.S. Intelligence Community. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **U.S. Intelligence Community**, build an institutional feedback-loop map with incentives, review points, and oversight hooks. Shape **U.S. Intelligence Community** work as a **requirements-to-product traceability ledger** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships replaces human review whenever evidence looks plausible.

Transfer task. Transfer **U.S. Intelligence Community** to a second module by preserving structured reasoning and source-integrity review, changing the source evidence, and naming a new reviewer.

6.2.2.2 Lesson 2: Declassified source-protection and institutional-control case study

Concept. Declassified source-protection and institutional-control case study uses attribution indicators cautiously by separating technical similarity, context, confidence, and geopolitical inference.

Why it matters. Without explicit treatment of **Declassified source-protection**, source laundering undermines structured reasoning and source-integrity review; the lesson builds the habit to separate reporting from inference, and inference from judgment.

Source support. Declassified source-protection and institutional-control case study rests on [297, 2026] and [298, 2026]. Its anchor reference records: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for the working definition that **Declassified source-protection and institutional-control case study** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. For **Declassified source-protection**, work from the cited evidence behind this row. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Declassified source-protection**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this structured reasoning and source-integrity review topic. The artifact must cite the declassified source descriptor, the bounded lesson about **Declassified source-protection and institutional-control case**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape **Declassified source-protection** work as a **requirements-to-product traceability ledger** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Apply this module's safe boundary for **Declassified source-protection** to another artifact while keeping structured reasoning and source-integrity review and reviewer ownership explicit.

6.2.2.3 Lesson 3: British Architecture: Declassified source-protection and institutional-control case study

Concept. British Architecture: Declassified source-protection and institutional-control case study studies the declassified record for institutional lessons about oversight, source protection, and limits on translating history into practice.

Why it matters. Without explicit treatment of **British Architecture**, source laundering undermines structured reasoning and source-integrity review; the lesson builds the habit to separate reporting from inference, and inference from judgment.

Source support. British Architecture: Declassified source-protection and institutional-control case study rests on [007, 2026]. The most specific cited work observes: It is SIS's task to pursue policy objectives by unorthodox means and to amass useful information. Use it for the working definition that **British Architecture: Declassified source-protection and institutional-control case study** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. Read **British Architecture** against the works cited for this row. [007, 2026] It is SIS's task to pursue policy objectives by unorthodox means and to amass useful information. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **British Architecture**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this structured reasoning and source-integrity review topic. The artifact must cite the declassified source descriptor, the bounded lesson about **British Architecture**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape **British Architecture** work as a **requirements-to-product traceability ledger** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Reuse the **British Architecture** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

6.2.2.4 Lesson 4: Israeli Architecture: Declassified source-protection and institutional-control case study

Concept. Israeli Architecture: Declassified source-protection and institutional-control case study studies the declassified record for institutional lessons about oversight, source protection, and limits on translating history into practice.

Why it matters. Israeli Architecture matters in the **Analytic Tradecraft and Source Integrity** lane because structured reasoning and source-integrity evidence must stay separate from judgment; source laundering is a common failure.

Source support. Israeli Architecture: Declassified source-protection and institutional-control case study rests on [008, 2026]. Its anchor reference records: An EBSCO Research Starter reference article on the Mossad, Israel's national intelligence agency established in 1949 and responsible for foreign intelligence collection and counterterrorism operations conducted outside Israel's borders. Use it for the working definition that **Israeli Architecture: Declassified source-protection and institutional-control case study** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. Ground **Israeli Architecture** in the evidence the row cites. [008, 2026] An EBSCO Research Starter reference article on the Mossad, Israel's national intelligence agency established in 1949 and responsible for foreign intelligence collection and counterterrorism operations conducted outside Israel's borders. It describes the agency's departmental structure (collection, political action and liaison, research, technology) and reviews historically documented operations including the 1960 capture of Adolf Eichmann and the rescue of Ethiopian Jews. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Israeli Architecture**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this structured reasoning and source-integrity review topic. The artifact must cite the declassified source descriptor, the bounded lesson about **Israeli Architecture**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape **Israeli Architecture** work as a **requirements-to-product traceability ledger** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Transfer **Israeli Architecture** from this module to a second motif by preserving structured reasoning and source-integrity review, replacing action with audit, and naming the blocked use.

6.2.2.5 Lesson 5: Chinese Architecture: MSS, PLA-SSF, United Front Work Department, APT Groups

Concept. Chinese Architecture: MSS, PLA-SSF, United Front Work Department, APT Groups studies APT reporting as attribution and confidence literacy: technical similarity, context, caveats, and geopolitical inference stay separate.

Why it matters. Without explicit treatment of **Chinese Architecture**, source laundering undermines structured reasoning and source-integrity review; the lesson builds the habit to separate reporting from inference, and inference from judgment.

Source support. Chinese Architecture: MSS, PLA-SSF, United Front Work Department, APT Groups rests on [009, 2026]. Its anchor reference records: A November 2023 report from MERICS (Mercator Institute for China Studies) analyzing Chinese state-affiliated cyber intrusions aimed at strategic goals. Use it for the claim that **Chinese Architecture: MSS, PLA-SSF, United Front Work Department, APT Groups** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. For **Chinese Architecture**, work from the cited evidence behind this row. [009, 2026] A November 2023 report from MERICS (Mercator Institute for China Studies) analyzing Chinese state-affiliated cyber intrusions aimed at strategic goals. It argues that Chinese actors pursue long-term, persistent access to European technology firms and critical infrastructure for espionage rather than disruption, with targeting aligned to government priorities such as semiconductors, pharmaceuticals, and advanced manufacturing. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Chinese Architecture**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this structured reasoning and source-integrity review topic. The artifact must name the source descriptor, the bounded claim about **Chinese Architecture**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Chinese Architecture** work as a **requirements-to-product traceability ledger** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that Chinese Architecture: MSS, PLA-SSF, United Front Work Department, APT Groups replaces human review whenever evidence looks plausible.

Transfer task. Transfer **Chinese Architecture** to a second module by preserving structured reasoning and source-integrity review, changing the source evidence, and naming a new reviewer.

6.2.2.6 Lesson 6: Five Eyes and Allied Intelligence Sharing: BRUSA to UKUSA

Concept. Five Eyes and Allied Intelligence Sharing: BRUSA to UKUSA uses the sharing arrangement to distinguish alliance governance, handling rules, legal authority, and source caveats.

Why it matters. Five Eyes and Allied Intelligence Sharing connects classroom vocabulary to Analytic Tradecraft and Source Integrity practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Five Eyes and Allied Intelligence Sharing: BRUSA to UKUSA rests on [010, 2026] and [011, 2026]. The lead source's own note reads: The collection traces the emergence and evolution of bilateral and multilateral agreements from the postwar era, including the BRUSA and UKUSA agreements, drawing on records from UK, US, and Australian agencies plus freedom-of-information releases. Use them for the claim that **Five Eyes and Allied Intelligence Sharing: BRUSA to UKUSA** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. Read **Five Eyes and Allied Intelligence Sharing** against the works cited for this row. [010, 2026] An online archive maintained by Unredacted UK that compiles declassified government documents on intelligence sharing among the Five Eyes nations (United States, United Kingdom, Canada, Australia, and New Zealand). The collection traces the emergence and evolution of bilateral and multilateral agreements from the postwar era, including the BRUSA and UKUSA agreements, drawing on records from UK, US, and Australian agencies plus freedom-of-information releases. [011, 2026] A curated collection from Unredacted UK presenting documents declassified by the NSA and GCHQ in 2010 relating

to US-UK signals intelligence cooperation. It covers the 1946 British-US Communications Agreement (BRUSA), its wartime origins from 1940, and its evolution into the 1956 UKUSA Agreement and the broader Five Eyes alliance. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Five Eyes and Allied Intelligence Sharing**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this structured reasoning and source-integrity review topic. The artifact must name the source descriptor, the bounded claim about **Five Eyes and Allied Intelligence**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Five Eyes and Allied Intelligence Sharing** work as a **requirements-to-product traceability ledger** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that Five Eyes and Allied Intelligence Sharing: BRUSA to UKUSA can be used while ignoring the rule to separate reporting from inference, and inference from judgment.

Transfer task. Transfer **Five Eyes and Allied Intelligence Sharing** to a second module by preserving structured reasoning and source-integrity review, changing the source evidence, and naming a new reviewer.

6.2.2.7 Lesson 7: Non-State Intelligence Actors: Terrorist, Criminal, PMC

Concept. Non-State Intelligence Actors: Terrorist, Criminal, PMC studies non-state actors through organizational indicators, funding patterns, and open-source evidence with strict minimization.

Why it matters. Non-State Intelligence Actors matters in the **Analytic Tradecraft and Source Integrity** lane because structured reasoning and source-integrity evidence must stay separate from judgment; source laundering is a common failure.

Source support. Non-State Intelligence Actors: Terrorist, Criminal, PMC rests on [012, 2026]. The lead source's own note reads: A Grey Dynamics analysis article (Rachel Brown, 2021) on how non-state actors conduct counterintelligence. Use it for fixing what **Non-State Intelligence Actors: Terrorist, Criminal, PMC** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. For **Non-State Intelligence Actors**, work from the cited evidence behind this row. [012, 2026] A Grey Dynamics analysis article (Rachel Brown, 2021) on how non-state actors conduct counterintelligence. It argues that although such groups lack the technical collection capabilities of states, they compensate through open-source and human-source methods and benefit defensively from compartmentalized, cell-based structures and ideological cohesion. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Non-State Intelligence Actors**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this structured reasoning and source-integrity review topic. The artifact must name the source descriptor, the bounded claim about **State Intelligence Actors**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Non-State Intelligence Actors** work as a **requirements-to-product traceability ledger** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that Non-State Intelligence Actors: Terrorist, Criminal, PMC is optional whenever separate reporting from inference, and inference from judgment feels inconvenient.

Transfer task. Transfer **Non-State Intelligence Actors** to a second module by preserving structured reasoning and source-integrity review, changing the source evidence, and naming a new reviewer.

6.2.2.8 Lesson 8: Fusion Centers, JITFs, and Inter-Agency Coordination

Concept. Fusion Centers, JITFs, and Inter-Agency Coordination applies Fusion, Centers, JITFs within Analytic Tradecraft and Source Integrity: learners use separate reporting from inference, and inference from judgment and structured reasoning and source-integrity review evidence before any judgment moves forward.

Why it matters. Analysts use **Fusion Centers, JITFs, and Inter-Agency Coordination** to separate reporting from inference, and inference from judgment. A defensible treatment names the judgment it enables for structured reasoning and source-integrity review, the proof limit that source laundering would otherwise hide, and the reviewer accountable for challenge.

Source support. Fusion Centers, JITFs, and Inter-Agency Coordination rests on [297, 2026] and [298, 2026]. The closest source to this row notes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for fixing what **Fusion Centers, JITFs, and Inter-Agency Coordination** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. For **Fusion Centers, JITFs, and Inter-Agency Coordination**, reason from the sources cited in this row. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Fusion Centers, JITFs, and Inter-Agency Coordination**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this structured reasoning and source-integrity review topic. The artifact must name the source descriptor, the bounded claim about **Fusion Centers JITFs and Inter-Agency**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape this subject work as a **requirements-to-product traceability ledger** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that Fusion Centers, JITFs, and Inter-Agency Coordination establishes intent without reviewing alternative explanations.

Transfer task. Transfer **Fusion Centers, JITFs, and Inter-Agency Coordination** to a second module by preserving structured reasoning and source-integrity review, changing the source evidence, and naming a new reviewer.

6.2.2.9 Lesson 9: Intelligence Oversight: Congressional, Judicial, Executive Mechanisms

Concept. Intelligence Oversight: Congressional, Judicial, Executive Mechanisms applies Oversight, Congressional, Judicial within Analytic Tradecraft and Source Integrity: learners use separate reporting from inference, and inference from judgment and structured reasoning and source-integrity review evidence before any judgment moves forward.

Why it matters. Intelligence Oversight matters in the **Analytic Tradecraft and Source Integrity** lane because structured reasoning and source-integrity evidence must stay separate from judgment; source laundering is a common failure.

Source support. Intelligence Oversight: Congressional, Judicial, Executive Mechanisms rests on [298, 2026] and [297, 2026]. Its anchor reference records: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for fixing what **Intelligence Oversight: Congressional, Judicial, Executive Mechanisms** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. For **Intelligence Oversight**, work from the cited evidence behind this row. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Intelligence Oversight**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this structured reasoning and source-integrity review topic. The artifact must name the source descriptor, the bounded claim about **Intelligence Oversight**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Intelligence Oversight** work as a **requirements-to-product traceability ledger** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that Intelligence Oversight: Congressional, Judicial, Executive Mechanisms replaces human review whenever evidence looks plausible.

Transfer task. Transfer **Intelligence Oversight** to a second module by preserving structured reasoning and source-integrity review, changing the source evidence, and naming a new reviewer.

6.2.3 Intelligence Community Architectures worked safe example: synthetic inputs, evidence, and review

Worked example: a synthetic analyst cell evaluates whether a benign supplier delay signals normal friction or elevated risk. [234, 2026]; [247, 2026].

Triangulation anchors. In module 2's worked-example section, directly verified anchors for the **Analytic Tradecraft and Source Integrity** lane include [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2026e]; [Agency, 2009]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **intelligence-cycle governance**. Learners use a **requirements-to-product traceability ledger** and keep this boundary visible: Activities stay inside public, synthetic, or instructor-provided materials and never become live collection or tasking.

Frame. The classroom question centers on **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships**. Excluded actions stay explicit, and the **Dissemination-and-Marking Control Lens** planning question is: Which audience, release authority, marking vocabulary, records duty, and feedback loop governs this intelligence artifact?

Inputs. For the **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships** scenario, use synthetic shipment notes, public policy excerpts, and a short instructor-provided event timeline. The Dissemination-and-Marking Control Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships**, students write hypotheses, list evidence for and against each, mark assumptions, and assign confidence only after alternatives are tested. Pause whenever an inference about U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships** classroom scenario; unit artifact = requirements-to-product traceability ledger; evidence = allowed inputs; method = structured reasoning and source-integrity review; output = an analytic note with a hypothesis table, confidence statement, dissent field, and collection gap list; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships** as "Dissemination-and-Marking Control Lens confirms it" is not enough. The revision ties the claim to structured reasoning and source-integrity review, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

6.2.4 Intelligence Community Architectures practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Dissemination-and-Marking Control Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**.

Triangulation anchors. In module 2's practice-sequence section, directly verified anchors for the **Analytic Tradecraft and Source Integrity** lane include [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2026e]; [Agency, 2009]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships, Declassified source-protection and institutional-control case study, British Architecture: Declassified source-protection and institutional-control case study; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Analytic Tradecraft and Source Integrity** lane.
2. Frame	Answer the lens question: Which audience, release authority, marking vocabulary, records duty, and feedback loop governs this intelligence artifact?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships: dissemination map with audience, caveat, marking, records, and feedback fields.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the requirements-to-product traceability ledger fields for U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships.	Unit profile note.	Evidence artifacts include requirement card, source descriptor.

Move	Learner action	Output	Check
4. Challenge	Test the misconception that U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships replaces human review whenever evidence looks plausible.	Failure-mode note.	The artifact applies the key distinction: separate reporting from inference, and inference from judgment.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

6.2.4.1 Intelligence Community Architectures instructor notes: source reasoning, review points, and studio focus Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**. [234, 2026]; [247, 2026].

6.2.4.2 Intelligence Community Architectures extension exercise: peer validation and refresh trigger review **Evidence anchor.** Section 6; [234, 2026].

Have learners swap artifacts and apply the **Dissemination-and-Marking Control Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**.

6.2.5 Intelligence Community Architectures knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 6; [234, 2026].

1. Explain how **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships** is defined here; name the source descriptor that supports the definition.
2. Contrast **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships** with **Declassified source-protection and institutional-control case study** using the **Dissemination-and-Marking Control Lens** artifact fields.
3. Identify one failure mode from the **Analytic Tradecraft and Source Integrity** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which assumption would change the judgment if it were false?
5. Correct this misconception: that U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships replaces human review whenever evidence looks plausible.

6.2.5.1 Intelligence Community Architectures answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships** without source evidence, uncertainty, or a safe transfer task.

6.3 Intelligence Community Architectures assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 6; [234, 2026].

6.3.1 Intelligence Community Architectures evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 6; [234, 2026].

6.3.2 Intelligence Community Architectures transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 6; [234, 2026].

6.3.2.1 Intelligence Community Architectures lineage and source tradition: profile, concepts, and first anchors This sits in the **Analytic Tradecraft and Source Integrity** lineage: turning uncertainty into reviewable judgment through sourcing, alternatives, separated likelihood and confidence language, warning indicators, and explicit analytic lineage. [234, 2026]; [247, 2026].

6.3.2.2 Intelligence Community Architectures working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 6; [234, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**, with provenance and reviewability throughout.

6.3.2.3 Intelligence Community Architectures knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** reporting, assumptions, alternatives, confidence language, dissent, and source descriptors. [234, 2026]; [247, 2026].
- **Transforms:** hypothesis generation, evidence sorting, assumption challenge, confidence calibration, and dissent capture.
- **Outputs:** analytic note, hypothesis table, assumption list, and confidence statement.
- **Failure modes:** single-hypothesis reasoning, source laundering, confidence inflation, and suppressed dissent.

6.3.2.4 Intelligence Community Architectures transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 6; [234, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**.
- **Evidence contract:** keep the **Analytic Tradecraft and Source Integrity** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as analytic note, hypothesis table, assumption list, and confidence statement that another reviewer can audit.

6.3.2.5 Intelligence Community Architectures profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 6; [234, 2026].

The matched profile emphasizes turning uncertainty into reviewable judgment through sourcing, alternatives, separated likelihood and confidence language, warning indicators, and explicit analytic lineage. The method stack is key assumptions check, analysis of competing hypotheses, diagnosticity review, indicators and warnings, probability calibration, red-team review, collective tradecraft rating, and source descriptor audit; the local topic cluster is **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**.

6.3.3 Intelligence Community Architectures evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 6; [234, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Analytic Tradecraft and Source Integrity** profile tells reviewers what evidence is strong enough for the module artifact built around **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**.

6.3.3.1 Intelligence Community Architectures guide source spine: inherited keys and local citation roles Primary guide citations: [234, 2026]; [247, 2026]; [249, 2026]; [276, 2026]; [277, 2026]; [284, 2026]; [288, 2026]; [289, 2026]; [293, 2026]; [006, 2026]; [007, 2026]; [008, 2026]; [009, 2026]; [010, 2026]; [011, 2026]; [012, 2026]; [297, 2026]; [298, 2026].

6.3.3.2 Intelligence Community Architectures verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [234, 2026]; [247, 2026].

Tier	What counts	How it is used
Source guide	[234, 2026]; [247, 2026]; [249, 2026]; [276, 2026]; [277, 2026]; [284, 2026]; [288, 2026]; [289, 2026]; [293, 2026]; [006, 2026]; [007, 2026]; [008, 2026]; [009, 2026]; [010, 2026]; [011, 2026]; [012, 2026]; [297, 2026]; [298, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 2's source-canon section, directly verified anchors for the **Analytic Tradecraft and Source Integrity** lane include [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2026e]; [Agency, 2009]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study** and [234, 2026]; [247, 2026], but only directly verified source URLs are encoded as citations.

6.3.3.3 Intelligence Community Architectures intelligence practice lens: evidence artifact and safety check Practice lens: **Dissemination-and-Marking Control Lens** for **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**. [234, 2026]; [247, 2026].

Planning question: Which audience, release authority, marking vocabulary, records duty, and feedback loop governs this intelligence artifact?

Evidence artifact: dissemination map with audience, caveat, marking, records, and feedback fields.

Validation rule: verify source authority, public/classification status, CAPCO-safe vocabulary, audience need, and records disposition before reuse. Applied to **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**.

Handoff contract: deliver release-neutral summaries, source metadata, marking rationale, and review ownership as separate fields.

Safety check: exclude classified content, live release decisions, source-method exposure, and improvised control markings.

6.3.3.4 Intelligence Community Architectures runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 6; [234, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	2.99	2.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Intelligence Community Architectures to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Bounded autonomy, procurement, incident-response, and assurance studio	2.101	2.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Intelligence Community Architectures	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Model-card, recoverability, retention, and learner-support evidence package	2.102	2.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Intelligence Community Architectures	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships	2.1	2.1 U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Declassified source-protection and institutional-control case study	2.2	2.2 source title transformed into safe curriculum treatment; original: Soviet/Russian Architecture: Cheka → GPU → NKVD → MGB → KGB → SVR/FSB/GRU	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Declassified source-protection and institutional-control case study	2.3	2.3 source title transformed into safe curriculum treatment; original: British Architecture: MI5, MI6/SIS, GCHQ, DI, JIC	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Declassified source-protection and institutional-control case study	2.4	2.4 source title transformed into safe curriculum treatment; original: Israeli Architecture: Mossad, Shin Bet, Unit 8200, LAKAM	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Chinese Architecture: MSS, PLA-SSF, United Front Work Department, APT Groups	2.5	2.5 Chinese Architecture: MSS, PLA-SSF, United Front Work Department, APT Groups	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Five Eyes and Allied Intelligence Sharing: BRUSA to UKUSA	2.6	2.6 Five Eyes and Allied Intelligence Sharing: BRUSA to UKUSA	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Non-State Intelligence Actors: Terrorist, Criminal, PMC	2.7	2.7 Non-State Intelligence Actors: Terrorist, Criminal, PMC	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Fusion Centers, JITFs, and Inter-Agency Coordination	2.8	2.8 Fusion Centers, JITFs, and Inter-Agency Coordination	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Intelligence Oversight: Congressional, Judicial, Executive Mechanisms	2.9	2.9 Intelligence Oversight: Congressional, Judicial, Executive Mechanisms	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence

6.3.3.5 Intelligence Community Architectures reusable subsection contract: topic rows, artifacts, and safety duties Evidence anchor. Section 6; [234, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Declassified source-protection and institutional-control case study	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
British Architecture: Declassified source-protection and institutional-control case study	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Israeli Architecture: Declassified source-protection and institutional-control case study	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Chinese Architecture: MSS, PLA-SSF, United Front Work Department, APT Groups	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Five Eyes and Allied Intelligence Sharing: BRUSA to UKUSA	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Non-State Intelligence Actors: Terrorist, Criminal, PMC	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence

Lesson topic	Practice lens	Evidence artifact	Safety check
Fusion Centers, JITFs, and Inter-Agency Coordination	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Intelligence Oversight: Congressional, Judicial, Executive Mechanisms	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence

6.3.3.6 Intelligence Community Architectures annotated source ledger: real titles and local contribution Each source cited by this **Analytic Tradecraft and Source Integrity** module is paired below with its real title and a one-line note on what it contributes to **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**.

Source	Cited work	What it contributes	Status
[234, 2026]	AI Act	The European Commission's official page on the AI Act, described as the first comprehensive legal framework on artificial intelligence worldwide. It explains the regulation's risk-based approach, classifying AI systems into unacceptable, high, transparency, and minimal risk tiers, with prohibited practices and strict requirements for high-risk uses.	verified source-guide
[247, 2026]	AI in the Public Sector	Official OECD.AI public-sector AI theme page.	original source-guide
[249, 2026]	GovTech: Putting People First	The official page for the World Bank's Global Program on GovTech and Public Sector Innovation, which helps governments use technology and data to improve public services and governance. It describes support for digital transformation in public administration across areas such as tax administration, public financial management, human resource systems, and citizen engagement, with cross-cutting themes including responsible AI and green digital transformation.	verified source-guide
[276, 2026]	What is a Data Protection Impact Assessment and When Is This Mandatory?	A European Data Protection Board FAQ page, part of its data protection guide for small businesses, explaining Data Protection Impact Assessments (DPIAs) and when they are mandatory. It describes a DPIA as a written assessment of the impact of a planned processing operation, required when processing poses high risks to individuals' rights.	verified source-guide
[277, 2026]	Endorsed WP29 Guidelines	This is a European Data Protection Board webpage listing guidelines and documents originating from the Article 29 Working Party that the EDPB endorsed at its first plenary meeting. The catalogued materials relate to the GDPR and cover topics such as consent and transparency, data breach notification, automated decision-making and profiling, data protection impact assessments, data protection officers, and binding corporate rules.	verified source-guide

Source	Cited work	What it contributes	Status
[284, 2026]	Verifiable Credential Data Integrity 1.0	The W3C Recommendation for Verifiable Credential Data Integrity 1.0, published May 2025, defining mechanisms for ensuring the authenticity and integrity of verifiable credentials using cryptographic proofs. It specifies a process of data transformation, hashing, and proof generation, and a corresponding verification procedure, along with a proof data model containing properties such as type, verification method, purpose, and proof value.	verified source-guide
[288, 2026]	Algorithmic Transparency Recording Standard Hub	A GOV.UK collection page serving as the hub for the UK Algorithmic Transparency Recording Standard (ATRS), maintained by the Government Digital Service. It provides a standardized template for documenting public-sector use of algorithmic tools, completion guidance, policy on scope and compliance, and a searchable repository of published transparency records.	verified source-guide
[289, 2026]	Guidance for Organisations Using the Algorithmic Transparency Recording Standard	This is a GOV.UK guidance page published by the Government Digital Service that instructs public sector organizations on completing the Algorithmic Transparency Recording Standard (ATRS) template and publishing their records to the GOV.UK repository. It applies both to central government bodies required to publish under mandatory policy and to other public sector bodies doing so voluntarily.	verified source-guide
[293, 2026]	Inventory of NARA Artificial Intelligence (AI) Use Cases	The National Archives and Records Administration (NARA) official inventory of its artificial intelligence use cases, documenting 14 projects across deployed, pilot, and planned stages. Deployed efforts include workplace productivity tools, automated tagging for museum experiences, and historical record retrieval, while pilots cover PII detection and redaction, semantic search, and metadata generation, and planned work targets FOIA processing and public search.	verified source-guide
[006, 2026]	Director of National Intelligence - Intelligence Community Directives	A Federation of American Scientists repository cataloguing the Intelligence Community Directives (ICDs) issued by the Director of National Intelligence. ICDs are the principal means by which the DNI provides policy, guidance, and direction to the U.S. Intelligence Community.	verified source-guide
[007, 2026]	THE FRIENDS BRITAIN'S POST-WAR SECRET INTELLIGENCE	It is SIS's task to pursue policy objectives by unorthodox means and to amass useful information.	original source-guide

Source	Cited work	What it contributes	Status
[008, 2026]	Mossad / Military History and Science	An EBSCO Research Starter reference article on the Mossad, Israel's national intelligence agency established in 1949 and responsible for foreign intelligence collection and counterterrorism operations conducted outside Israel's borders. It describes the agency's departmental structure (collection, political action and liaison, research, technology) and reviews historically documented operations including the 1960 capture of Adolf Eichmann and the rescue of Ethiopian Jews.	verified source-guide
[009, 2026]	"Here to stay" – Chinese state-affiliated hacking for strategic goals	A November 2023 report from MERICS (Mercator Institute for China Studies) analyzing Chinese state-affiliated cyber intrusions aimed at strategic goals. It argues that Chinese actors pursue long-term, persistent access to European technology firms and critical infrastructure for espionage rather than disruption, with targeting aligned to government priorities such as semiconductors, pharmaceuticals, and advanced manufacturing.	verified source-guide
[010, 2026]	The Five Eyes Archive	An online archive maintained by Unredacted UK that compiles declassified government documents on intelligence sharing among the Five Eyes nations (United States, United Kingdom, Canada, Australia, and New Zealand). The collection traces the emergence and evolution of bilateral and multilateral agreements from the postwar era, including the BRUSA and UKUSA agreements, drawing on records from UK, US, and Australian agencies plus freedom-of-information releases.	verified source-guide
[011, 2026]	BRUSA and UKUSA Agreements: GCHQ and NSA	A curated collection from Unredacted UK presenting documents declassified by the NSA and GCHQ in 2010 relating to US-UK signals intelligence cooperation. It covers the 1946 British-US Communications Agreement (BRUSA), its wartime origins from 1940, and its evolution into the 1956 UKUSA Agreement and the broader Five Eyes alliance.	verified source-guide
[012, 2026]	Counterintelligence Activities of Non-State Actors - Grey Dynamics	A Grey Dynamics analysis article (Rachel Brown, 2021) on how non-state actors conduct counterintelligence. It argues that although such groups lack the technical collection capabilities of states, they compensate through open-source and human-source methods and benefit defensively from compartmentalized, cell-based structures and ideological cohesion.	verified source-guide
[297, 2026]	Intelligence Community Directive 203: Analytic Standards	Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products.	original source-guide
[298, 2026]	Intelligence Community Directives	Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations.	original source-guide

Where this sits. This module's overview is Section 6; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

6.3.4 Intelligence Community Architectures governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 6; [234, 2026].

6.3.5 Intelligence Community Architectures analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 2's governance-boundary section, directly verified anchors for the **Analytic Tradecraft and Source Integrity** lane include [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2026e]; [Agency, 2009]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **Analytic Tradecraft and Source Integrity** for **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**. [234, 2026]; [247, 2026].

Curriculum topic spine: U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships, **Declassified source-protection and institutional-control case study**, **British Architecture: Declassified source-protection and institutional-control case study**. **Verified anchor cluster:** [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2026e]; [Agency, 2009]; [for the Study of Intelligence, 2002]; [for the Study of Intelligence, 1994]; [Agency, 2016].

Conceptual depth: turning uncertainty into reviewable judgment through sourcing, alternatives, separated likelihood and confidence language, warning indicators, and explicit analytic lineage.

Method stack: key assumptions check, analysis of competing hypotheses, diagnosticity review, indicators and warnings, probability calibration, red-team review, collective tradecraft rating, and source descriptor audit.

Composability contract: every agent output must preserve evidence, assumptions, judgments, likelihood, confidence, dissent, empirical limits, and change history as separable fields.

Known failure modes: source laundering, automation bias, hidden assumptions, collapsed likelihood/confidence language, hindsight certainty, SAT-as-bias-cure overclaiming, and visually persuasive but weakly sourced claims.

Defensive boundary: analysis remains educational and decision-supportive; it does not become tasking, targeting, covert collection, or policy advocacy. Applied to **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**.

Anchor	Why it matters here
[of the Director of National Intelligence, 2015]	Official ODNI analytic tradecraft standards directive. Checked as of 2026-05-21; role: source_quality_anchor.
[of the Director of National Intelligence, 2026d]	Official sourcing directive for traceability, citations, source descriptors, and source summaries. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026e]	Official ODNI explanation of analytic objectivity, ombuds, and tradecraft standards. Checked as of 2026-05-21; role: curriculum_anchor.
[Agency, 2009]	Official structured analytic techniques primer for bias checks, alternatives, and warning analysis. Checked as of 2026-05-21; role: curriculum_anchor.
[for the Study of Intelligence, 2002]	Official CIA Center for the Study of Intelligence essay on Kent's professionalization of intelligence analysis and analytic standards. Checked as of 2026-06-11; role: curriculum_anchor.
[for the Study of Intelligence, 1994]	Official CIA CSI republication of Kent's final essay on analyst-policy relations, warning, intention, and communication boundaries. Checked as of 2026-06-11; role: curriculum_anchor.
[Agency, 2016]	Defense intelligence structured-analysis primer for classroom analytic exercises. Checked as of 2026-05-21; role: curriculum_anchor.

6.3.5.1 Intelligence Community Architectures evidence standard and citation floor: source families and discovery limits Official guidance supplies governance, safety, and legal constraints for the **Analytic Tradecraft and Source Integrity** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [234, 2026]; [247, 2026].

6.3.6 Intelligence Community Architectures agentic boundary: assist, approve, block, and record

Evidence anchor. Section 6; [234, 2026].

AGEINT translation is bounded by the **Analytic Tradecraft and Source Integrity** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**.

6.3.6.1 Intelligence Community Architectures permitted defensive utility: curriculum uses and safe outputs **Evidence anchor.** Section 6; [234, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**.

6.3.6.2 Intelligence Community Architectures excluded operational boundary: blocked actions and stop rules Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [234, 2026]; [247, 2026] and **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

6.3.7 Intelligence Community Architectures governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 6; [234, 2026].

Governance is practiced as a gate on the **Analytic Tradecraft and Source Integrity** lane. Learners use the **Dissemination-and-Marking Control Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**.

6.3.7.1 Intelligence Community Architectures governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [234, 2026]; [247, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Analytic Tradecraft and Source Integrity** failure modes and the **Dissemination-and-Marking Control Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

6.3.7.2 Intelligence Community Architectures evidence package handoff: appendices, records, and reuse **Evidence anchor.** Section 6; [234, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Dissemination-and-Marking Control Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**.

6.3.7.3 Intelligence Community Architectures current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**. [234, 2026]; [247, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_odni_icd_203` for **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**?	Intelligence Community Directive 203: Analytic Standards; lane `source_quality_spine`; checked 2026-05-21.	dissemination map with audience, caveat, marking, records, and feedback fields; Official ODNI analytic tradecraft standards directive.
What does the module inherit from `official_odni_icd_206` for **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**?	Intelligence Community Directive 206: Sourcing Requirements for Disseminated Analytic Products; lane `analytic_tradecraft`; checked 2026-05-21.	dissemination map with audience, caveat, marking, records, and feedback fields; Official sourcing directive for traceability, citations, source descriptors, and source summaries.
What does the module inherit from `official_odni_objectivity` for **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**?	Objectivity and IC Analytic Standards; lane `analytic_tradecraft`; checked 2026-05-21.	dissemination map with audience, caveat, marking, records, and feedback fields; Official ODNI explanation of analytic objectivity, ombuds, and tradecraft standards.
What does the module inherit from `official_cia_tradecraft_primer` for **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**?	A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis; lane `analytic_tradecraft`; checked 2026-05-21.	dissemination map with audience, caveat, marking, records, and feedback fields; Official structured analytic techniques primer for bias checks, alternatives, and warning analysis.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 6; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

6.3.8 Intelligence Community Architectures assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 6; [234, 2026].

6.3.9 Intelligence Community Architectures assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 6; [234, 2026].

6.3.9.1 Intelligence Community Architectures capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study** and [234, 2026]; [247, 2026].

6.3.9.2 Intelligence Community Architectures instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study** and [234, 2026]; [247, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

6.3.9.3 Intelligence Community Architectures assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships	Completed **dissemination map with audience, caveat, marking, records, and feedback fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Declassified source-protection and institutional-control case study	Completed **dissemination map with audience, caveat, marking, records, and feedback fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
British Architecture: Declassified source-protection and institutional-control case study	Completed **dissemination map with audience, caveat, marking, records, and feedback fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

6.3.10 Intelligence Community Architectures refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [234, 2026]; [247, 2026] and **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**.

6.3.10.1 Intelligence Community Architectures refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**. The local signals begin with [234, 2026]; [247, 2026].

6.3.10.2 Intelligence Community Architectures claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**, and the source spine for these checks begins with [234, 2026]; [247, 2026].

6.3.11 Intelligence Community Architectures reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [234, 2026]; [247, 2026].

Triangulation anchors. In module 2's review-checklist section, directly verified anchors for the **Analytic Tradecraft and Source Integrity** lane include [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2026e]; [Agency, 2009]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study**. [234, 2026]; [247, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

6.3.12 Intelligence Community Architectures learning-path links: module map, overview, and curriculum atlas

Follow the cross-links to move between **U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships; Declassified source-protection and institutional-control case study** and the rest of the curriculum without losing the source spine: orientation first, then the parent unit, then the modules on either side. Primary sources: [234, 2026]; [247, 2026].

Section 2, Section 4, Section 5, Section 7

7 Tradecraft: Core Principles

7.0.1 Tradecraft: Core Principles figures and course links: visual evidence, source flow, and navigation

The module uses Figure 35 and Figure 30 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 4, Section 6, Section 8.
This module teaches the **Governed Intelligence Cycle and Dissemination Architecture** lane through a bounded, source-backed coursebook chapter. [237, 2026]; [266, 2026].

7.1 Governed Intelligence Cycle and Dissemination Architecture frame for Tradecraft: Core Principles: source context, topic focus, and reader task

Evidence anchor. Section 7; [237, 2026].

7.1.1 Tradecraft: Core Principles orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 7; [237, 2026].

7.1.2 Tradecraft: Core Principles conceptual primer: source context, core model, and reader task

This chapter teaches analytic tradecraft as disciplined judgment under uncertainty: claims become useful only when evidence, assumptions, alternatives, confidence, and dissent remain visible. The chapter uses **Structured-Judgment Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance**.
The central distinction is to separate reporting from inference, and inference from judgment. Core topics include **What Is Tradecraft? Historical Definitions and Evolution; Operations security (OPSEC) governance; Compartmentation and need-to-know governance**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Community, 2026]; [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026c]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [237, 2026]; [266, 2026].
Learners move from vocabulary and the **Structured-Judgment Lens** distinction through topic lessons on **What Is Tradecraft? Historical Definitions and Evolution** with evidence and misconception checks, then assemble an **analytic note with hypotheses, evidence table, confidence, and dissent fields** with safety and rights gates.

7.1.3 Tradecraft: Core Principles learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 7; [237, 2026].

- Connect **What Is Tradecraft? Historical Definitions and Evolution and Operations security (OPSEC) governance** to **Governed Intelligence Cycle and Dissemination Architecture** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build an **analytic note with hypotheses, evidence table, confidence, and dissent fields** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate reporting from inference, and inference from judgment; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as cycle theater, undocumented dissemination, classification drift, unclear release authority, stale records assumptions, and feedback loops that hide bias, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: cycle and marking material remains public-source and educational; it never handles classified content, live release decisions, or source-method exposure.

7.1.4 Tradecraft: Core Principles core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 7; [237, 2026].

Term	Working definition
Source descriptor	a compact statement of where evidence came from and what it can support
Assumption	a claim accepted for analysis that still needs challenge
Alternative hypothesis	a plausible explanation that competes with the favored account
Confidence	a calibrated expression of evidentiary strength and analytic uncertainty
Dissent	a documented disagreement that preserves minority reasoning for review
What Is Tradecraft? Historical Definitions and…	Key terms: What, Is, Tradecraft.
Operations security (OPSEC) governance	Key terms: Operations, security, OPSEC.

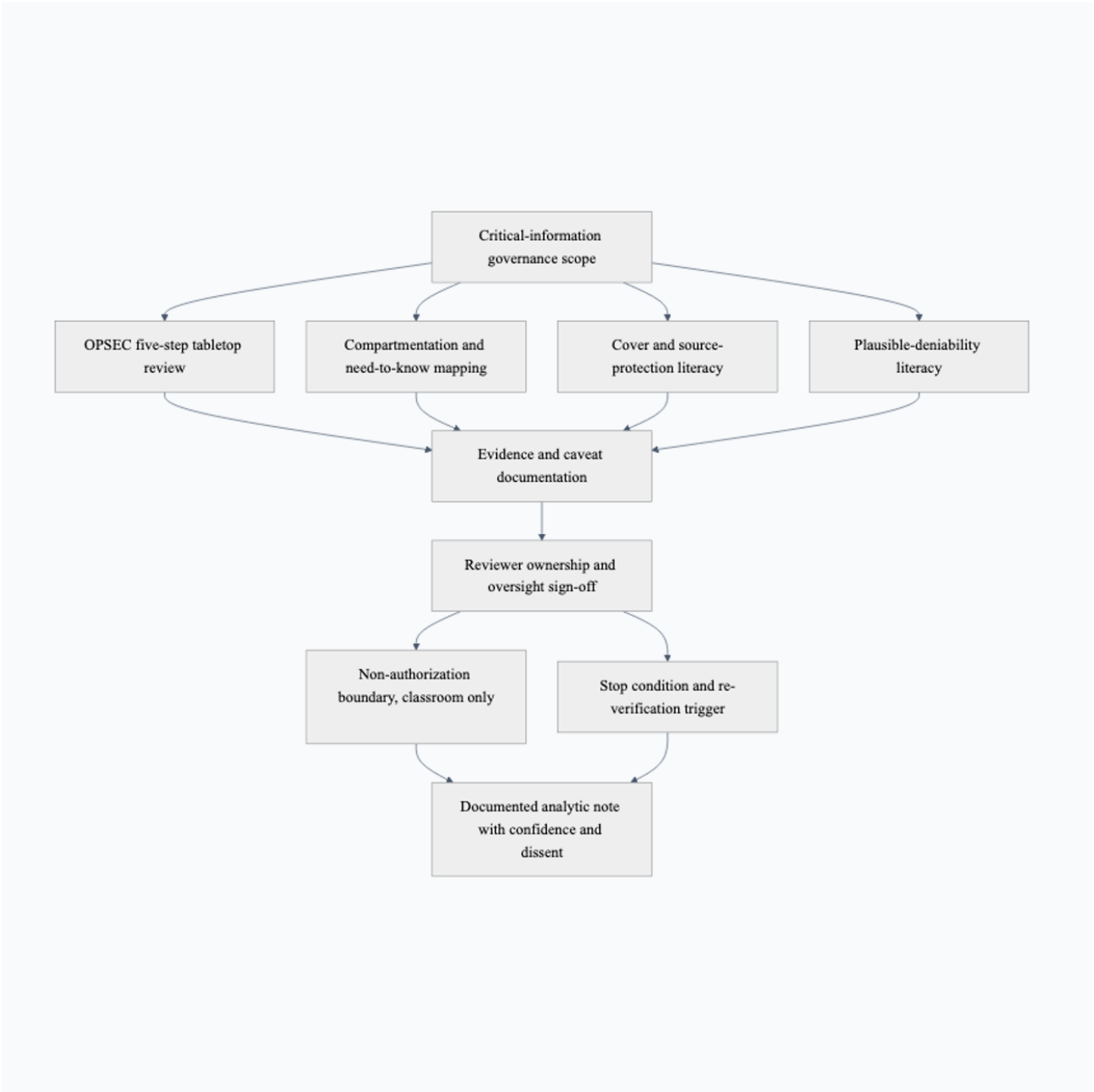


Figure 35: How core tradecraft concepts are taught as documented governance controls feeding analytic oversight, not as operational activity. It is anchored to the foundations of intelligence tradecraft / tradecraft core principles section; use it to inspect Critical-information governance scope, OPSEC five-step tabletop review, Compartmentation and need-to-know mapping, and Cover and source-protection literacy while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

7.2 Structured-Judgment Lens path for Tradecraft: Core Principles: lesson cluster, safe artifact, and review

Evidence anchor. Section 7; [237, 2026].

7.2.1 Tradecraft: Core Principles practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 7; [237, 2026].

7.2.2 Tradecraft: Core Principles topic lessons: source-backed concepts and transfer tasks

This module builds analytic tradecraft as disciplined judgment under uncertainty: claims become useful only when evidence, assumptions, alternatives, confidence, and dissent remain visible. The sequence opens with **What Is Tradecraft? Historical Definitions and Evolution**, **Operations security (OPSEC) governance**, **Compartmentation and need-to-know governance** and applies the **Structured-Judgment Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 30; module overview Section 7; curriculum atlas Section 2.

Triangulation anchors. In module 3's topic-lessons section, directly verified anchors for the **Governed Intelligence Cycle and Dissemination Architecture** lane include [Community, 2026]; [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026c]; [of the Director of National Intelligence, 2025a]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

7.2.2.1 Lesson 1: What Is Tradecraft? Historical Definitions and Evolution

Concept. What Is Tradecraft? Historical Definitions and Evolution treats operational tradecraft as governance: OPSEC, compartmentation, cover discipline, and oversight—not contact or evasion activity.

Why it matters. Analysts use **What Is Tradecraft? Historical Definitions** to separate reporting from inference, and inference from judgment. A defensible treatment names the judgment it enables for structured reasoning and source-integrity review, the proof limit that confusing governance vocabulary with operational authorization would otherwise hide, and the reviewer accountable for challenge.

Source support. What Is Tradecraft? Historical Definitions and Evolution rests on [013, 2026] and [014, 2026]. The closest source to this row notes: It surveys core disciplines such as surveillance and counter-surveillance, cover and disguise, technical and human intelligence work, and the field's evolution toward digital and cyber methods. Use them for fixing what **What Is Tradecraft? Historical Definitions and Evolution** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2015].

Evidence to inspect. For **What Is Tradecraft? Historical Definitions**, work from the cited evidence behind this row. [013, 2026] This is an instructional training document hosted on Scribd that introduces the fundamentals of intelligence tradecraft, defined as the methods and skills used in intelligence operations. It covers core concepts and types of tradecraft, cover and operational security, casing and surveillance, clandestine communication, and information gathering. [014, 2026] An educational article from TRDCRFT defining tradecraft as the techniques, strategies, and tools used by intelligence operatives to pursue objectives while maintaining secrecy and operational security. It surveys core disciplines such as surveillance and counter-surveillance, cover and disguise, technical and human intelligence work, and the field's evolution toward digital and cyber methods. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **What Is Tradecraft? Historical Definitions**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must name the governance descriptor, the bounded claim about **What Is Tradecraft Historical Definitions**, the compartmentation caveat, the uncertainty note, the non-authorization boundary, and the reviewer who signs oversight. Shape **What Is Tradecraft? Historical Definitions** work as a **requirements-to-product traceability ledger** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **What Is Tradecraft? Historical Definitions**: that governance vocabulary about tradecraft confers operational authorization rather than the constraints under which any action must be approved.

Transfer task. Reuse the **What Is Tradecraft? Historical Definitions** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

7.2.2.2 Lesson 2: Operations security (OPSEC) governance

Concept. Operations security (OPSEC) governance applies the five-step OPSEC process—identify critical information, analyze threats, analyze vulnerabilities, assess risk, apply countermeasures—in tabletop governance review only.

Why it matters. Analysts use **Operations security (OPSEC) governance** to separate reporting from inference, and inference from judgment. A defensible treatment names the judgment it enables for structured reasoning and source-integrity review, the proof limit that confusing governance vocabulary with operational authorization would otherwise hide, and the reviewer accountable for challenge.

Source support. Operations security (OPSEC) governance rests on [297, 2026] and [298, 2026]. The closest source to this row notes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for pinning down the scope of **Operations security (OPSEC) governance**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2015].

Evidence to inspect. Read **Operations security (OPSEC) governance** against the works cited for this row. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Operations security (OPSEC) governance**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must name the governance descriptor, the bounded claim about **Operations security governance**, the compartmentation caveat, the uncertainty note, the non-authorization boundary, and the reviewer who signs oversight. Shape this subject work as a **requirements-to-product traceability ledger** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Operations security (OPSEC) governance**: that governance vocabulary about tradecraft confers operational authorization rather than the constraints under which any action must be approved.

Transfer task. Reuse the **Operations security (OPSEC) governance** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

7.2.2.3 Lesson 3: Compartmentation and need-to-know governance

Concept. Compartmentation and need-to-know governance maps compartment boundaries, access lists, and need-to-know fields before any information moves across teams.

Why it matters. Compartmentation and need-to-know governance connects classroom vocabulary to Governed Intelligence Cycle and Dissemination Architecture practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Compartmentation and need-to-know governance rests on [297, 2026] and [298, 2026]. The most specific cited work observes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for the claim that **Compartmentation and need-to-know governance** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2015].

Evidence to inspect. For **Compartmentation and need-to-know governance**, reason from the sources cited in this row. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. Build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must name the governance descriptor, the bounded claim about **Compartmentation and need-to-know governance**, the compartmentation caveat, the uncertainty note, the non-authorization boundary, and the reviewer who signs oversight. Shape this subject work as a **requirements-to-product traceability ledger** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Compartmentation and need-to-know governance**: that governance vocabulary about tradecraft confers operational authorization rather than the constraints under which any action must be approved.

Transfer task. Reuse the **Compartmentation and need-to-know governance** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

7.2.2.4 Lesson 4: Cover and legend governance literacy

Concept. Cover and legend governance literacy — Review cover-and-legend governance as oversight, documentation, and source-protection literacy—not identity fabrication.

Why it matters. Cover and legend governance literacy matters in the **Governed Intelligence Cycle and Dissemination Architecture** lane because structured reasoning and source-integrity evidence must stay separate from judgment; confusing governance vocabulary with operational authorization is a common failure.

Source support. Cover and legend governance literacy rests on [015, 2026]. The closest source to this row notes: It distinguishes official cover (diplomatic channels, immunity) from non-official cover (no government acknowledgment, less protection). Use it for the claim that **Cover and legend governance literacy** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2015].

Evidence to inspect. For **Cover and legend governance literacy**, reason from the sources cited in this row. [015, 2026] A Wikipedia article explaining the concept of cover in human intelligence and counterintelligence work, defined as the ostensible identity assumed by a covert agent. It distinguishes official cover (diplomatic channels, immunity) from non-official cover (no government acknowledgment, less protection). The article surveys historical examples of front organizations and assumed identities. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. Build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must name the governance descriptor, the bounded claim about **Cover and legend governance literacy**, the compartmentation caveat, the uncertainty note, the non-authorization boundary, and the reviewer who signs oversight. Shape this subject work as a **requirements-to-product traceability ledger** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Cover and legend governance literacy**: that governance vocabulary about tradecraft confers operational authorization rather than the constraints under which any action must be approved.

Transfer task. Apply this module's safe boundary for **Cover and legend governance literacy** to another artifact while keeping structured reasoning and source-integrity review and reviewer ownership explicit.

7.2.2.5 Lesson 5: The Principle of Plausible Deniability

Concept. The Principle of Plausible Deniability treats operational tradecraft as governance: OPSEC, compartmentation, cover discipline, and oversight—not contact or evasion activity.

Why it matters. Analysts use **The Principle of Plausible Deniability** to separate reporting from inference, and inference from judgment. A defensible treatment names the judgment it enables for structured reasoning and source-integrity review, the proof limit that confusing governance vocabulary with operational authorization would otherwise hide, and the reviewer accountable for challenge.

Source support. The Principle of Plausible Deniability rests on [297, 2026] and [298, 2026]. The most specific cited work observes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for the claim that **The Principle of Plausible Deniability** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2015].

Evidence to inspect. For **The Principle of Plausible Deniability**, work from the cited evidence behind this row. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **The Principle**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must name the governance descriptor, the bounded claim about **Principle of Plausible Deniability**, the compartmentation caveat, the uncertainty note, the non-authorization boundary, and the reviewer who signs oversight. Shape **The Principle of Plausible Deniability** work as a **requirements-to-product traceability ledger** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **The Principle of Plausible Deniability**: that governance vocabulary about tradecraft confers operational authorization rather than the constraints under which any action must be approved.

Transfer task. Apply this module's safe boundary for **The Principle of Plausible Deniability** to another artifact while keeping structured reasoning and source-integrity review and reviewer ownership explicit.

7.2.2.6 Lesson 6: Claim-ledger memory exercise that tracks evidence changes rather than people

Concept. Claim-ledger memory exercise that tracks evidence changes rather than people connects cognitive science claims to analytic bias literacy: what the brain prioritizes, what it misses, and how review compensates.

Why it matters. Claim-ledger memory exercise that tracks evidence changes rather than people connects classroom vocabulary to Governed Intelligence Cycle and Dissemination Architecture practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Claim-ledger memory exercise that tracks evidence changes rather than people rests on [016, 2026]. Its anchor reference records: Place where victim can be controlled with limited avenues of escape. Use it for fixing what **Claim-ledger memory exercise that tracks evidence changes rather than people** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2015].

Evidence to inspect. Ground **Claim-ledger memory exercise that tracks evidence changes rather than people** in the evidence the row cites. [016, 2026] Place where victim can be controlled with limited avenues of escape. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Claim-ledger memory exercise that tracks evidence changes rather than people**, build a claim-ledger memory card with source descriptor, source-change event, retention rule, contamination check, and reviewer disposition; it must not track real people, assets, or behavioral patterns. Shape this subject work as a **requirements-to-product traceability ledger** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that a current record reflects the original, when undocumented changes to evidence over time can silently rewrite what is remembered.

Transfer task. Transfer **Claim-ledger memory exercise that tracks evidence changes rather than people** from this module to a second motif by preserving structured reasoning and source-integrity review, replacing action with audit, and naming the blocked use.

7.2.2.7 Lesson 7: Situational Awareness: Urban and Rural Tradecraft

Concept. Situational Awareness: Urban and Rural Tradecraft treats operational tradecraft as governance: OPSEC, compartmentation, cover discipline, and oversight—not contact or evasion activity.

Why it matters. Situational Awareness connects classroom vocabulary to Governed Intelligence Cycle and Dissemination Architecture practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Situational Awareness: Urban and Rural Tradecraft rests on [014, 2026]. The most specific cited work observes: An educational article from TRDCRFT defining tradecraft as the techniques, strategies, and tools used by intelligence operatives to pursue objectives while maintaining secrecy and operational security. Use it for pinning down the scope of **Situational Awareness: Urban and Rural Tradecraft**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2015].

Evidence to inspect. For **Situational Awareness**, work from the cited evidence behind this row. [014, 2026] An educational article from TRDCRFT defining tradecraft as the techniques, strategies, and tools used by intelligence operatives to pursue objectives while maintaining secrecy and operational security. It surveys core disciplines such as surveillance and counter-surveillance, cover and disguise, technical and human intelligence work, and the field's evolution toward digital and cyber methods. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Situational Awareness**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must name the governance descriptor, the bounded claim about **Situational Awareness**, the compartmentation caveat, the uncertainty note, the non-authorization boundary, and the reviewer who signs oversight. Shape **Situational Awareness** work as a **requirements-to-product traceability ledger** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Situational Awareness**: that governance vocabulary about tradecraft confers operational authorization rather than the constraints under which any action must be approved.

Transfer task. Reuse the **Situational Awareness** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

7.2.2.8 Lesson 8: Code Words, Glossaries, and the Language of Espionage

Concept. Code Words, Glossaries, and the Language of Espionage treats operational tradecraft as governance: OPSEC, compartmentation, cover discipline, and oversight—not contact or evasion activity.

Why it matters. Code Words, Glossaries, and the Language of Espionage matters in the **Governed Intelligence Cycle and Dissemination Architecture** lane because structured reasoning and source-integrity evidence must stay separate from judgment; confusing governance vocabulary with operational authorization is a common failure.

Source support. Code Words, Glossaries, and the Language of Espionage rests on [017, 2026]. The lead source's own note reads: An educational glossary from the International Spy Museum, a nonprofit institution in Washington, DC, presenting an alphabetized dictionary of espionage terminology. Use it for the claim that **Code Words, Glossaries, and the Language of Espionage** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2015].

Evidence to inspect. Ground **Code Words, Glossaries, and the Language of Espionage** in the evidence the row cites. [017, 2026] An educational glossary from the International Spy Museum, a nonprofit institution in Washington, DC, presenting an alphabetized dictionary of espionage terminology. It defines operational roles (agent, handler, case officer), intelligence disciplines such as HUMINT, SIGINT, and IMINT, major organizations (CIA, FBI, KGB, MI5, MI6, NSA), and historical equipment like the Enigma machine and U-2 aircraft. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Code Words, Glossaries, and the Language of Espionage**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must name the governance descriptor, the bounded claim about **Code Words Glossaries and the**, the compartmentation caveat, the uncertainty note, the non-authorization boundary, and the reviewer who signs oversight. Shape this subject work as a **requirements-to-product traceability ledger** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Code Words, Glossaries, and the Language of Espionage**: that governance vocabulary about tradecraft confers operational authorization rather than the constraints under which any action must be approved.

Transfer task. Apply this module's safe boundary for **Code Words, Glossaries, and the Language of Espionage** to another artifact while keeping structured reasoning and source-integrity review and reviewer ownership explicit.

7.2.2.9 Lesson 9: Historical clandestine-communications ethics

Concept. Historical clandestine-communications ethics uses the historical motif to discuss source-protection ethics, documentation, and oversight without recreating handling procedures.

Why it matters. Analysts use **Historical clandestine-communications ethics** to separate reporting from inference, and inference from judgment. A defensible treatment names the judgment it enables for structured reasoning and source-integrity review, the proof limit that cycle theater would otherwise hide, and the reviewer accountable for challenge.

Source support. Historical clandestine-communications ethics rests on [018, 2026], [005, 2026], and [019, 2026]. The closest source to this row notes: 1, March 2026). Use them for fixing what **Historical clandestine-communications ethics** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2015].

Evidence to inspect. For **Historical clandestine-communications ethics**, work from the cited evidence behind this row. [018, 2026] A Nextgov article reporting on an essay in the CIA's Studies in Intelligence journal by RAND researcher Thomas Mulligan. It argues that as AI makes deepfakes and synthetic communications easier, trust in digital channels erodes, paradoxically increasing the value of traditional human intelligence methods. [005, 2026] A blog post on SemperVerus summarizing a CIA Studies in Intelligence article, "Espionage in Our AI Future: Why Human Intelligence Still Matters" (Vol. 70, No. 1, March 2026). It argues that as AI makes technical intelligence cheaper and AI-driven fabrication more pervasive, human intelligence becomes relatively more valuable, since human specialists are needed to verify source reliability over time. [019, 2026] By Thomas Mulligan, a researcher at the RAND Corporation who served in CIA during 2008–14. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. Build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must cite the historical descriptor, the bounded lesson about **Historical clandestine-communications**

ethics, the handling caveat, the uncertainty note, the protected-tradecraft boundary, and the reviewer who clears the account. Shape this subject work as a **requirements-to-product traceability ledger** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Historical clandestine-communications ethics**: that a documented handling precedent licenses repeating the approach, rather than a case-bound record whose risks must be re-assessed each time.

Transfer task. Apply this module's safe boundary for **Historical clandestine-communications ethics** to another artifact while keeping structured reasoning and source-integrity review and reviewer ownership explicit.

7.2.3 Tradecraft: Core Principles worked safe example: synthetic inputs, evidence, and review

Worked example: a synthetic analyst cell evaluates whether a benign supplier delay signals normal friction or elevated risk. [237, 2026]; [266, 2026].

Triangulation anchors. In module 3's worked-example section, directly verified anchors for the **Governed Intelligence Cycle and Dissemination Architecture** lane include [Community, 2026]; [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026c]; [of the Director of National Intelligence, 2025a]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **intelligence-cycle governance**. Learners use a **requirements-to-product traceability ledger** and keep this boundary visible: Activities stay inside public, synthetic, or instructor-provided materials and never become live collection or tasking.

Frame. The classroom question centers on **What Is Tradecraft? Historical Definitions and Evolution**. Excluded actions stay explicit, and the **Structured-Judgment Lens** planning question is: Which assumptions, alternatives, confidence statements, and source limits must stay visible for review?

Inputs. For the **What Is Tradecraft? Historical Definitions and Evolution** scenario, use synthetic shipment notes, public policy excerpts, and a short instructor-provided event timeline. The Structured-Judgment Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **What Is Tradecraft? Historical Definitions and Evolution**, students write hypotheses, list evidence for and against each, mark assumptions, and assign confidence only after alternatives are tested. Pause whenever an inference about What Is Tradecraft? Historical Definitions and Evolution appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **What Is Tradecraft? Historical Definitions and Evolution** classroom scenario; unit artifact = requirements-to-product traceability ledger; evidence = allowed inputs; method = structured reasoning and source-integrity review; output = an analytic note with a hypothesis table, confidence statement, dissent field, and collection gap list; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **What Is Tradecraft? Historical Definitions and Evolution** as "Structured-Judgment Lens confirms it" is not enough. The revision ties the claim to structured reasoning and source-integrity review, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **What Is Tradecraft? Historical Definitions and Evolution** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

7.2.4 Tradecraft: Core Principles practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Structured-Judgment Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance**.

Triangulation anchors. In module 3's practice-sequence section, directly verified anchors for the **Governed Intelligence Cycle and Dissemination Architecture** lane include [Community, 2026]; [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026c]; [of the Director of National Intelligence, 2025a]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare What Is Tradecraft? Historical Definitions and Evolution, Operations security governance, Compartmentation and need-to-know governance; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Governed Intelligence Cycle and Dissemination Architecture** lane.
2. Frame	Answer the lens question: Which assumptions, alternatives, confidence statements, and source limits must stay visible for review?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for What Is Tradecraft? Historical Definitions and Evolution: analytic note with hypotheses, evidence table, confidence, and dissent fields.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the requirements-to-product traceability ledger fields for What Is Tradecraft? Historical Definitions and Evolution.	Unit profile note.	Evidence artifacts include requirement card, source descriptor.
4. Challenge	Test the misconception that governance vocabulary about tradecraft confers operational authorization rather than the constraints under which any action must be approved.	Failure-mode note.	The artifact applies the key distinction: separate reporting from inference, and inference from judgment.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

7.2.4.1 Tradecraft: Core Principles instructor notes: source reasoning, review points, and studio focus Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance**. [237, 2026]; [266, 2026].

7.2.4.2 Tradecraft: Core Principles extension exercise: peer validation and refresh trigger review

Evidence anchor. Section 7; [237, 2026].

Have learners swap artifacts and apply the **Structured-Judgment Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance**.

7.2.5 Tradecraft: Core Principles knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 7; [237, 2026].

1. Explain how **What Is Tradecraft? Historical Definitions and Evolution** is defined here; name the source descriptor that supports the definition.
2. Contrast **What Is Tradecraft? Historical Definitions and Evolution** with **Operations security governance** using the **Structured-Judgment Lens** artifact fields.
3. Identify one failure mode from the **Governed Intelligence Cycle and Dissemination Architecture** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which assumption would change the judgment if it were false?
5. Correct this misconception: that governance vocabulary about tradecraft confers operational authorization rather than the constraints under which any action must be approved.

7.2.5.1 Tradecraft: Core Principles answer quality rubric: source evidence, uncertainty, and safe transfer

Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **What Is Tradecraft? Historical Definitions and Evolution** without source evidence, uncertainty, or a safe transfer task.

7.3 Tradecraft: Core Principles assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 7; [237, 2026].

7.3.1 Tradecraft: Core Principles evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 7; [237, 2026].

7.3.2 Tradecraft: Core Principles transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 7; [237, 2026].

7.3.2.1 Tradecraft: Core Principles lineage and source tradition: profile, concepts, and first anchors This sits in the **Governed Intelligence Cycle and Dissemination Architecture** lineage: treating the intelligence cycle as a governed information system whose collection, processing, analysis, dissemination, evaluation, marking, and records obligations stay explicit. [237, 2026]; [266, 2026].

7.3.2.2 Tradecraft: Core Principles working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 7; [237, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance**, with provenance and reviewability throughout.

7.3.2.3 Tradecraft: Core Principles knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** requirements, audience needs, public-source evidence, caveats, and feedback signals. [237, 2026]; [266, 2026].
- **Transforms:** requirement framing, collection scoping, source evaluation, analytic judgment, dissemination, and feedback review.
- **Outputs:** release-neutral brief, audience map, caveat register, and feedback note.
- **Failure modes:** unscoped audiences, missing caveats, weak records, and product reuse without feedback.

7.3.2.4 Tradecraft: Core Principles transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 7; [237, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance**.
- **Evidence contract:** keep the **Governed Intelligence Cycle and Dissemination Architecture** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as release-neutral brief, audience map, caveat register, and feedback note that another reviewer can audit.

7.3.2.5 Tradecraft: Core Principles profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 7; [237, 2026].

The matched profile emphasizes treating the intelligence cycle as a governed information system whose collection, processing, analysis, dissemination, evaluation, marking, and records obligations stay explicit. The method stack is cycle mapping, priority-to-product traceability, data-lifecycle mapping, classification vocabulary review, dissemination-caveat audit, customer feedback, and oversight checkpointing; the local topic cluster is **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance**.

7.3.3 Tradecraft: Core Principles evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 7; [237, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Governed Intelligence Cycle and Dissemination Architecture** profile tells reviewers what evidence is strong enough for the module artifact built around **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance**.

7.3.3.1 Tradecraft: Core Principles guide source spine: inherited keys and local citation roles Primary guide citations: [237, 2026]; [266, 2026]; [269, 2026]; [278, 2026]; [279, 2026]; [283, 2026]; [290, 2026]; [291, 2026]; [294, 2026]; [013, 2026]; [014, 2026]; [015, 2026]; [016, 2026]; [017, 2026]; [018, 2026]; [005, 2026]; [019, 2026]; [297, 2026]; [298, 2026].

7.3.3.2 Tradecraft: Core Principles verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [237, 2026]; [266, 2026].

Tier	What counts	How it is used
Source guide	[237, 2026]; [266, 2026]; [269, 2026]; [278, 2026]; [279, 2026]; [283, 2026]; [290, 2026]; [291, 2026]; [294, 2026]; [013, 2026]; [014, 2026]; [015, 2026]; [016, 2026]; [017, 2026]; [018, 2026]; [005, 2026]; [019, 2026]; [297, 2026]; [298, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 3's source-canon section, directly verified anchors for the **Governed Intelligence Cycle and Dissemination Architecture** lane include [Community, 2026]; [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026c]; [of the Director of National Intelligence, 2025a]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance** and [237, 2026]; [266, 2026], but only directly verified source URLs are encoded as citations.

7.3.3.3 Tradecraft: Core Principles intelligence practice lens: evidence artifact and safety check Practice lens: **Structured-Judgment Lens** for **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance**. [237, 2026]; [266, 2026].

Planning question: Which assumptions, alternatives, confidence statements, and source limits must stay visible for review?

Evidence artifact: analytic note with hypotheses, evidence table, confidence, and dissent fields.

Validation rule: separate raw reporting, inference, judgment, and recommendation before synthesis. Applied to **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance**.

Handoff contract: handoff preserves alternatives, uncertainty, caveats, and revision history for downstream modules.

Safety check: avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence.

7.3.3.4 Tradecraft: Core Principles runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 7; [237, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	3.99	3.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Tradecraft: Core Principles to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Bounded autonomy, procurement, incident-response, and assurance studio	3.101	3.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Tradecraft: Core Principles	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Model-card, recoverability, retention, and learner-support evidence package	3.102	3.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Tradecraft: Core Principles	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
What Is Tradecraft? Historical Definitions and Evolution	3.1	3.1 What Is Tradecraft? Historical Definitions and Evolution	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Operations security (OPSEC) governance	3.2	3.2 source title transformed into safe curriculum treatment; original: Operational Security (OPSEC): Process and the Five-Step Method	AI/Data Accountability Lens	AI/data impact card with authority, provenance, model version, impact score, register status, human owner, and review cadence	reject automated adverse action, hidden surveillance expansion, unowned outputs, unreviewed model drift, and opaque downstream reuse
Compartmentation and need-to-know governance	3.3	3.3 source title transformed into safe curriculum treatment; original: Compartmentation: Need-to-Know vs. Need-to-Share	AI/Data Accountability Lens	AI/data impact card with authority, provenance, model version, impact score, register status, human owner, and review cadence	reject automated adverse action, hidden surveillance expansion, unowned outputs, unreviewed model drift, and opaque downstream reuse
Cover and legend governance literacy	3.4	3.4 source title transformed into safe curriculum treatment; original: Cover: Official, Non-Official Cover (NOC), Deep Cover, Legends	AI/Data Accountability Lens	AI/data impact card with authority, provenance, model version, impact score, register status, human owner, and review cadence	reject automated adverse action, hidden surveillance expansion, unowned outputs, unreviewed model drift, and opaque downstream reuse
The Principle of Plausible Deniability	3.5	3.5 The Principle of Plausible Deniability	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Claim-ledger memory exercise that tracks evidence changes rather than people	3.6	3.6 source title transformed into safe curriculum treatment; original: Pattern-of-Life Analysis and How to Disrupt It	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Situational Awareness: Urban and Rural Tradecraft	3.7	3.7 Situational Awareness: Urban and Rural Tradecraft	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Code Words, Glossaries, and the Language of Espionage	3.8	3.8 Code Words, Glossaries, and the Language of Espionage	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Historical clandestine-communications ethics	3.9	3.9 source title transformed into safe curriculum treatment; original: Return of Classical Tradecraft in the AI Era: Dead Drops, Brush Passes, In-Person Exchanges	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence

7.3.3.5 Tradecraft: Core Principles reusable subsection contract: topic rows, artifacts, and safety duties Evidence anchor. Section 7; [237, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
What Is Tradecraft? Historical Definitions and Evolution	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Operations security (OPSEC) governance	AI/Data Accountability Lens	AI/data impact card with authority, provenance, model version, impact score, register status, human owner, and review cadence	reject automated adverse action, hidden surveillance expansion, unowned outputs, unreviewed model drift, and opaque downstream reuse
Compartmentation and need-to-know governance	AI/Data Accountability Lens	AI/data impact card with authority, provenance, model version, impact score, register status, human owner, and review cadence	reject automated adverse action, hidden surveillance expansion, unowned outputs, unreviewed model drift, and opaque downstream reuse
Cover and legend governance literacy	AI/Data Accountability Lens	AI/data impact card with authority, provenance, model version, impact score, register status, human owner, and review cadence	reject automated adverse action, hidden surveillance expansion, unowned outputs, unreviewed model drift, and opaque downstream reuse
The Principle of Plausible Deniability	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence

Lesson topic	Practice lens	Evidence artifact	Safety check
Claim-ledger memory exercise that tracks evidence changes rather than people	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Situational Awareness: Urban and Rural Tradecraft	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Code Words, Glossaries, and the Language of Espionage	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Historical clandestine-communications ethics	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence

7.3.3.6 Tradecraft: Core Principles annotated source ledger: real titles and local contribution Each source cited by this **Governed Intelligence Cycle and Dissemination Architecture** module is paired below with its real title and a one-line note on what it contributes to **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance**.

Source	Cited work	What it contributes	Status
[237, 2026]	Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities	Official GAO AI accountability framework.	original source-guide
[266, 2026]	PROV Overview	A W3C Working Group Note from 2013 that provides an overview and roadmap for the PROV family of specifications for representing and exchanging provenance information on the web. It defines provenance as information about the entities, activities, and people involved in producing data, used to assess quality, reliability, and trustworthiness.	verified source-guide
[269, 2026]	Data on the Web Best Practices	A W3C Recommendation, "Data on the Web Best Practices," published January 31, 2017 by the Data on the Web Best Practices Working Group. It offers 35 best practices for publishing and consuming data on the Web, covering metadata, licensing and provenance, data quality, dataset versioning, persistent URIs, machine-readable formats, vocabulary reuse, access methods, preservation, and feedback.	verified source-guide
[278, 2026]	Recommendation of the Council on Public Procurement	The OECD Recommendation of the Council on Public Procurement (OECD/LEGAL/0411), a legal instrument adopted by the OECD Council in 2015 on the proposal of the Public Governance Committee. It frames public procurement as a pillar of strategic governance and service delivery and sets out principles for governments to follow.	verified source-guide
[279, 2026]	Open Contracting Data Standard	The documentation homepage for the Open Contracting Data Standard, version 1.1.5, maintained by the Open Contracting Partnership to support disclosure of government contracting data across the procurement lifecycle. It provides a common data model spanning planning, tender, award, contract, and implementation stages, along with a primer, implementation guidance, technical schemas, and validation tooling.	verified source-guide

Source	Cited work	What it contributes	Status
[283, 2026]	Recommendation of the Council on Open Government	An OECD legal instrument document reproducing the Recommendation of the Council on Open Government (OECD/LEGAL/0438), adopted on 14 December 2017. It defines open government as a culture of governance promoting transparency, integrity, accountability, and stakeholder participation in support of democracy and inclusive growth.	verified source-guide
[290, 2026]	NIST SP 800-218A: Secure Software Development Practices for Generative AI and Dual-Use Foundation Models	NIST Special Publication 800-218A (July 2024), which augments the Secure Software Development Framework with practices specific to AI model development across the software lifecycle. Produced in response to Executive Order 14110, it addresses AI model producers, developers building on those models, and acquirers of AI systems, and is designed to be used alongside NIST SP 800-218.	verified source-guide
[291, 2026]	Revised 508 Standards and 255 Guidelines	Official documentation from the U.S. Access Board on the Revised 508 Standards and 255 Guidelines for information and communication technology accessibility. It establishes mandatory accessibility requirements for federal agencies and voluntary guidelines for telecommunications manufacturers, covering hardware, software, websites, electronic documents, and support services.	verified source-guide
[294, 2026]	M-25-21: Accelerating Federal Use of AI through Innovation, Governance, and Public Trust	An April 2025 Office of Management and Budget memorandum (M-25-21) directing executive branch agencies on federal use of artificial intelligence. Issued under Executive Order 14179, it instructs agencies to accelerate adoption of AI to improve public services and government efficiency while maintaining safeguards for civil rights, civil liberties, and privacy.	verified source-guide
[013, 2026]	Intelligence Tradecraft Overview / PDF / Surveillance	This is an instructional training document hosted on Scribd that introduces the fundamentals of intelligence tradecraft, defined as the methods and skills used in intelligence operations. It covers core concepts and types of tradecraft, cover and operational security, casing and surveillance, clandestine communication, and information gathering.	verified source-guide context; do not use as primary analytic support
[014, 2026]	Tradecraft: Covert Operative Tactics and Techniques	An educational article from TRDCRFT defining tradecraft as the techniques, strategies, and tools used by intelligence operatives to pursue objectives while maintaining secrecy and operational security. It surveys core disciplines such as surveillance and counter-surveillance, cover and disguise, technical and human intelligence work, and the field's evolution toward digital and cyber methods.	verified source-guide

Source	Cited work	What it contributes	Status
[015, 2026]	Cover (intelligence gathering)	A Wikipedia article explaining the concept of cover in human intelligence and counterintelligence work, defined as the ostensible identity assumed by a covert agent. It distinguishes official cover (diplomatic channels, immunity) from non-official cover (no government acknowledgment, less protection). The article surveys historical examples of front organizations and assumed identities.	verified source-guide context; do not use as primary analytic support
[016, 2026]	Surveillance Detection - State.gov	Place where victim can be controlled with limited avenues of escape.	original source-guide
[017, 2026]	Language of Espionage / International Spy Museum	An educational glossary from the International Spy Museum, a nonprofit institution in Washington, DC, presenting an alphabetized dictionary of espionage terminology. It defines operational roles (agent, handler, case officer), intelligence disciplines such as HUMINT, SIGINT, and IMINT, major organizations (CIA, FBI, KGB, MI5, MI6, NSA), and historical equipment like the Enigma machine and U-2 aircraft.	verified source-guide
[018, 2026]	Old-school spycraft could make a comeback as AI undermines trust	A Nextgov article reporting on an essay in the CIA's Studies in Intelligence journal by RAND researcher Thomas Mulligan. It argues that as AI makes deepfakes and synthetic communications easier, trust in digital channels erodes, paradoxically increasing the value of traditional human intelligence methods.	verified source-guide
[005, 2026]	CIA: Studies in AI and Human Intelligence - SemperVerus	A blog post on SemperVerus summarizing a CIA Studies in Intelligence article, "Espionage in Our AI Future: Why Human Intelligence Still Matters" (Vol. 70, No. 1, March 2026). It argues that as AI makes technical intelligence cheaper and AI-driven fabrication more pervasive, human intelligence becomes relatively more valuable, since human specialists are needed to verify source reliability over time.	verified source-guide
[019, 2026]	Espionage in Our AI Future: Why Human Intelligence Still Matters - CSI	By Thomas Mulligan, a researcher at the RAND Corporation who served in CIA during 2008–14.	original source-guide
[297, 2026]	Intelligence Community Directive 203: Analytic Standards	Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products.	original source-guide
[298, 2026]	Intelligence Community Directives	Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations.	original source-guide

Where this sits. This module's overview is Section 7; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

7.3.4 Tradecraft: Core Principles governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 7; [237, 2026].

7.3.5 Tradecraft: Core Principles analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 3's governance-boundary section, directly verified anchors for the **Governed Intelligence Cycle and Dissemination Architecture** lane include [Community, 2026]; [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026c]; [of the Director of National Intelligence, 2025a]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **Analytic Tradecraft and Source Integrity** for **What Is Tradecraft? Historical Definitions and Evolution; Operations security (OPSEC) governance**. [237, 2026]; [266, 2026].

Curriculum topic spine: What Is Tradecraft? Historical Definitions and Evolution, **Operations security (OPSEC) governance**, **Compartmentation and need-to-know governance**. **Verified anchor cluster:** [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2026e]; [Agency, 2009]; [for the Study of Intelligence, 2002]; [for the Study of Intelligence, 1994]; [Agency, 2016].

Conceptual depth: turning uncertainty into reviewable judgment through sourcing, alternatives, separated likelihood and confidence language, warning indicators, and explicit analytic lineage.

Method stack: key assumptions check, analysis of competing hypotheses, diagnosticity review, indicators and warnings, probability calibration, red-team review, collective tradecraft rating, and source descriptor audit.

Composability contract: every agent output must preserve evidence, assumptions, judgments, likelihood, confidence, dissent, empirical limits, and change history as separable fields.

Known failure modes: source laundering, automation bias, hidden assumptions, collapsed likelihood/confidence language, hindsight certainty, SAT-as-bias-cure overclaiming, and visually persuasive but weakly sourced claims.

Defensive boundary: analysis remains educational and decision-supportive; it does not become tasking, targeting, covert collection, or policy advocacy. Applied to **What Is Tradecraft? Historical Definitions and Evolution; Operations security (OPSEC) governance**.

Anchor	Why it matters here
[of the Director of National Intelligence, 2015]	Official ODNI analytic tradecraft standards directive. Checked as of 2026-05-21; role: source_quality_anchor.
[of the Director of National Intelligence, 2026d]	Official sourcing directive for traceability, citations, source descriptors, and source summaries. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026e]	Official ODNI explanation of analytic objectivity, ombuds, and tradecraft standards. Checked as of 2026-05-21; role: curriculum_anchor.
[Agency, 2009]	Official structured analytic techniques primer for bias checks, alternatives, and warning analysis. Checked as of 2026-05-21; role: curriculum_anchor.
[for the Study of Intelligence, 2002]	Official CIA Center for the Study of Intelligence essay on Kent's professionalization of intelligence analysis and analytic standards. Checked as of 2026-06-11; role: curriculum_anchor.
[for the Study of Intelligence, 1994]	Official CIA CSI republication of Kent's final essay on analyst-policy relations, warning, intention, and communication boundaries. Checked as of 2026-06-11; role: curriculum_anchor.
[Agency, 2016]	Defense intelligence structured-analysis primer for classroom analytic exercises. Checked as of 2026-05-21; role: curriculum_anchor.

7.3.5.1 Tradecraft: Core Principles evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **Governed Intelligence Cycle and Dissemination Architecture** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [237, 2026]; [266, 2026].

7.3.6 Tradecraft: Core Principles agentic boundary: assist, approve, block, and record

Evidence anchor. Section 7; [237, 2026].

AGEINT translation is bounded by the **Governed Intelligence Cycle and Dissemination Architecture** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance**.

7.3.6.1 Tradecraft: Core Principles permitted defensive utility: curriculum uses and safe outputs

Evidence anchor. Section 7; [237, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance**.

7.3.6.2 Tradecraft: Core Principles excluded operational boundary: blocked actions and stop rules

Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [237, 2026]; [266, 2026] and **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

7.3.7 Tradecraft: Core Principles governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 7; [237, 2026].

Governance is practiced as a gate on the **Governed Intelligence Cycle and Dissemination Architecture** lane. Learners use the **Structured-Judgment Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance**.

7.3.7.1 Tradecraft: Core Principles governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [237, 2026]; [266, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Governed Intelligence Cycle and Dissemination Architecture** failure modes and the **Structured-Judgment Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

7.3.7.2 Tradecraft: Core Principles evidence package handoff: appendices, records, and reuse

Evidence anchor. Section 7; [237, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Structured-Judgment Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance**.

7.3.7.3 Tradecraft: Core Principles current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance**. [237, 2026]; [266, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_intelligence_gov_how_ic_works` for **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance**?	How the IC Works; lane `governed_intelligence_cycle`; checked 2026-05-21.	analytic note with hypotheses, evidence table, confidence, and dissent fields; Official public explanation of the intelligence cycle, collection disciplines, dissemination, evaluation, oversight, and partners.
What does the module inherit from `official_odni_icd_203` for **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance**?	Intelligence Community Directive 203: Analytic Standards; lane `source_quality_spine`; checked 2026-05-21.	analytic note with hypotheses, evidence table, confidence, and dissent fields; Official ODNI analytic tradecraft standards directive.
What does the module inherit from `official_odni_icd_204` for **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance**?	Intelligence Community Directive 204: National Intelligence Priorities Framework; lane `collection_management`; checked 2026-05-21.	analytic note with hypotheses, evidence table, confidence, and dissent fields; Official prioritization directive for translating national intelligence priorities into collection, analysis, risk management, and responsiveness evaluation.
What does the module inherit from `official_odni_icd_504` for **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance**?	Intelligence Community Directive 504: Intelligence Community Data Management; lane `ai_ethics_data_governance`; checked 2026-05-21.	analytic note with hypotheses, evidence table, confidence, and dissent fields; Official IC data-management directive for data governance, data stewardship, CDO authority, interoperability, and data lifecycle management.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 7; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

7.3.8 Tradecraft: Core Principles assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 7; [237, 2026].

7.3.9 Tradecraft: Core Principles assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 7; [237, 2026].

7.3.9.1 Tradecraft: Core Principles capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance**. Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance** and [237, 2026]; [266, 2026].

7.3.9.2 Tradecraft: Core Principles instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance** and [237, 2026]; [266, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

7.3.9.3 Tradecraft: Core Principles assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
What Is Tradecraft? Historical Definitions and Evolution	Completed **analytic note with hypotheses, evidence table, confidence, and dissent fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Operations security (OPSEC) governance	Completed **analytic note with hypotheses, evidence table, confidence, and dissent fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Compartmentation and need-to-know governance	Completed **analytic note with hypotheses, evidence table, confidence, and dissent fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

7.3.10 Tradecraft: Core Principles refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [237, 2026]; [266, 2026] and **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance**.

7.3.10.1 Tradecraft: Core Principles refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance**. The local signals begin with [237, 2026]; [266, 2026].

7.3.10.2 Tradecraft: Core Principles claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance**, and the source spine for these checks begins with [237, 2026]; [266, 2026].

7.3.11 Tradecraft: Core Principles reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [237, 2026]; [266, 2026].
Triangulation anchors. In module 3's review-checklist section, directly verified anchors for the **Governed Intelligence Cycle and Dissemination Architecture** lane include [Community, 2026]; [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026c]; [of the Director of National Intelligence, 2025a]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance**. [237, 2026]; [266, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

7.3.12 Tradecraft: Core Principles learning-path links: module map, overview, and curriculum atlas

Follow the cross-links to move between **What Is Tradecraft? Historical Definitions and Evolution; Operations security governance** and the rest of the curriculum without losing the source spine: orientation first, then the parent unit, then the modules on either side. Primary sources: [237, 2026]; [266, 2026].
Section 2, Section 4, Section 6, Section 8

8 HUMAN INTELLIGENCE (HUMINT)

8.1 HUMAN INTELLIGENCE (HUMINT) learning spine and source route: unit purpose, module order, and evidence handoff

Evidence anchor. Section 8; [238, 2026].

8.1.1 human-source literacy and source protection discipline spine: domain question and learning focus

Evidence anchor. Section 8; [238, 2026].
This unit teaches **human-source literacy and source protection**. HUMINT lessons focus on motivation literacy, validation, consent, source risk, debrief hygiene, and oversight without teaching contact handling.

8.1.2 human-source literacy and source protection source-use contract: citation roles and evidence limits

Evidence anchor. Section 8; [238, 2026].
Use guide citations for HUMINT vocabulary and official oversight anchors for source-risk, minimization, and governance claims.

8.1.3 human-source literacy and source protection practice artifact: recurring packet and retained evidence

Evidence anchor. Section 8; [238, 2026].
The recurring practice artifact is a **source-risk and validation ethics worksheet** that draws on validation note, pressure-risk checklist, source-protection boundary, and oversight escalation memo. The unit keeps its learning spine explicit. Learners distinguish motivation frameworks from authorization, identify validation limits, and route sensitive concerns to oversight.

8.1.4 human-source literacy and source protection safety boundary: accountable, synthetic, and evidence-bounded limits

No elicitation, impersonation, covert contact, or operational source-management procedures; all cases use classroom fixtures.
This unit introduces the part's governing question, evidence artifacts, source-support spine, and capstone thread before the individual modules begin. [238, 2026]; [239, 2026].
Learners carry one unit capstone thread through the part: define an accountable intelligence question, bind it to source-quality constraints, produce a reviewable artifact, test the artifact against failure modes, and hand it off with enough context for another analyst or instructor to audit. The capstone remains public, synthetic, or owned-lab throughout; its first source anchors are [238, 2026]; [239, 2026].
This unit's deliverables are a source-canon card, claim/evidence ledger, safe-practice lab packet, failure-mode note, instructor rubric, and debrief memo. The full source-lane and evidence-package ledgers appear in the orientation and appendices; this unit introduction keeps only the learner-facing spine for [238, 2026]; [239, 2026].
This unit's safety gates are scope authorization, rights review, data provenance, tool allowlisting, human oversight, rollback, and evidence-bounded output. A missing gate turns the activity into a tabletop, audit, or written governance exercise until the gate is restored against [238, 2026]; [239, 2026].
Capstone thread:

Phase	Artifact	Review gate
Question	accountable learning question and excluded-action list	instructor confirms scope, allowed data, and rights impact
Source canon	source-lane map with guide citations, verified anchors, and refresh dates	citation keys resolve and source identity lock remains stable
Evidence ledger	claim, evidence, uncertainty, confidence, and reviewer register	every material claim has a source, caveat, and owner
Safe lab	synthetic or public dataset packet, tool allowlist, and stop conditions	no live target, private data, external action, or unsafe cyber-physical step
Assurance	evaluation rubric, failure-mode drill, rights map, and remediation note	human reviewer signs off before presentation or reuse
Debrief	capstone memo with lessons, residual risk, refresh triggers, and handoff owner	all unresolved questions and future approvals are explicit

Research lane: Collection Management and Multi-INT Requirements Discipline. Core anchors: [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]. Conceptual focus: requirements-driven, authority-bounded collection where priorities, legal basis, minimization, source protection, and evaluation are explicit. Composability contract: requirements, authorities, source disciplines, collection notes, retention limits, caveats, and evaluation metrics remain separable. **Practice lens:** Requirements-to-Evidence Lens; What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit? [238, 2026]; [239, 2026].

8.1.5 HUMAN INTELLIGENCE (HUMINT) visual navigation and module map: evidence flow, order, and safety cues

The unit uses Figure 36 and Figure 37 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 7, Section 9.

8.1.6 HUMAN INTELLIGENCE (HUMINT) module roster and source-lane inventory: citations, lanes, and learner route

Module	Section reference	Source spine
Agent Recruitment	Section 9	[238, 2026]; [239, 2026]; [240, 2026]; [280, 2026]; [281, 2026]; [282, 2026]; [292, 2026]; [295, 2026]; [296, 2026]; [020, 2026]; [021, 2026]; [298, 2026]; [297, 2026]; [022, 2026]; [023, 2026]; [024, 2026]; [004, 2026].
Agent Handling and Management	Section 10	[239, 2026]; [240, 2026]; [241, 2026]; [273, 2026]; [276, 2026]; [285, 2026]; [286, 2026]; [290, 2026]; [294, 2026]; [025, 2026]; [029, 2026]; [004, 2026]; [026, 2026]; [016, 2026]; [027, 2026]; [028, 2026]; [030, 2026]; [031, 2026]; [032, 2026].

Module	Section reference	Source spine
Source Protection and CI Integration	Section 11	[238, 2026]; [241, 2026]; [266, 2026]; [274, 2026]; [278, 2026]; [280, 2026]; [287, 2026]; [288, 2026]; [295, 2026]; [307, 2026]; [305, 2026]; [304, 2026]; [029, 2026]; [033, 2026]; [019, 2026]; [034, 2026].

Figure 36: The unit module map traces the part's chapters as a linear reading sequence. In the human intelligence humint section, it lets readers compare 3 module nodes in the unit's ordered, source-backed reading sequence from its first module to its last so the visual functions as a traceable course aid rather than an unscoped assertion.

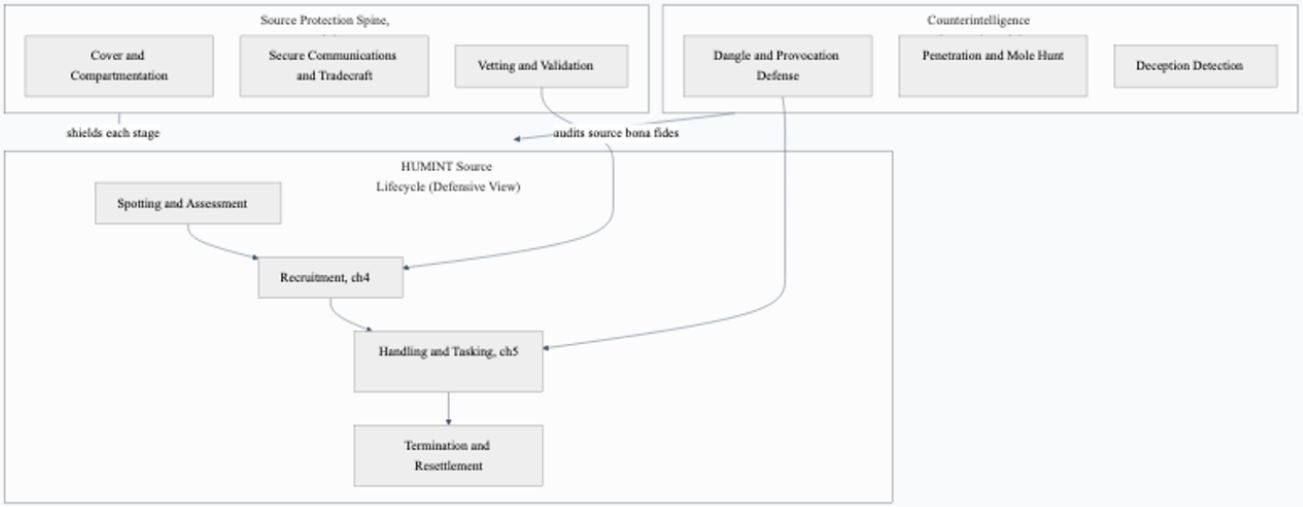


Figure 37: Part II presents HUMINT defensively as a managed source lifecycle (recruitment ch4, handling ch5) wrapped by a source-protection spine and continuous counterintelligence validation (ch6). It is anchored to the human intelligence humint section; use it to inspect HUMINT Source Lifecycle (Defensive View), Spotting and Assessment, Recruitment, ch4, and Handling and Tasking, ch5 while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

9 Agent Recruitment

9.0.1 Agent Recruitment figures and course links: visual evidence, source flow, and navigation

The module uses Figure 38 and Figure 36 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 8, Section 10.
This module teaches the **Collection Management and Multi-INT Requirements Discipline** lane through a bounded, source-backed coursebook chapter. [238, 2026]; [239, 2026].

9.1 Collection Management and Multi-INT Requirements Discipline frame for Agent Recruitment: source context, topic focus, and reader task

Evidence anchor. Section 9; [238, 2026].

9.1.1 Agent Recruitment orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 9; [238, 2026].

9.1.2 Agent Recruitment conceptual primer: source context, core model, and reader task

This chapter teaches collection management as requirements discipline: a source method is considered only after the priority, authority, minimization rule, source risk, and evaluation plan are explicit. The chapter uses **Requirements-to-Evidence Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**.
The central distinction is to separate collection discipline concepts from operational recruitment, interception, or tasking procedures. Core topics include **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy; Spotting indicators literacy for recruitment-risk**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [238, 2026]; [239, 2026].
Learners move from vocabulary and the **Requirements-to-Evidence Lens** distinction through topic lessons on **MICE Framework for recruitment-risk literacy** with evidence and misconception checks, then assemble a **requirements matrix with source descriptors, caveats, and collection limits** with safety and rights gates.

9.1.3 Agent Recruitment learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 9; [238, 2026].

- Connect **MICE Framework for recruitment-risk literacy and MICE Expanded: MICE Framework for recruitment-risk literacy** to **Collection Management and Multi-INT Requirements Discipline** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **requirements matrix with source descriptors, caveats, and collection limits** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate collection discipline concepts from operational recruitment, interception, or tasking procedures; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as opportunistic collection, priority drift, over-collection, weak minimization, source exposure, and confusing availability with authority, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: collection material remains doctrinal and governance-oriented; it does not teach recruitment, interception, surveillance, or tasking procedures.

9.1.4 Agent Recruitment core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 9; [238, 2026].

Term	Working definition
Priority	the relative importance of an intelligence question
Source discipline	a broad evidence channel such as HUMINT, SIGINT, GEOINT, OSINT, or FININT
Minimization	the rule that limits acquisition, retention, or use of unnecessary information
Source protection	the duty to reduce risk to people, methods, and sensitive relationships
Evaluation	the feedback step that tests whether the evidence satisfied the requirement
Gray-zone indicator	an observable signal of ambiguous coercion below armed conflict thresholds
Proxy pattern	a relationship suggesting indirect sponsorship without confirmed operational control
MICE Framework for recruitment-risk literacy	Key terms: MICE, Framework, recruitment.
MICE Expanded: MICE Framework for…	Key terms: MICE, Expanded, MICE.

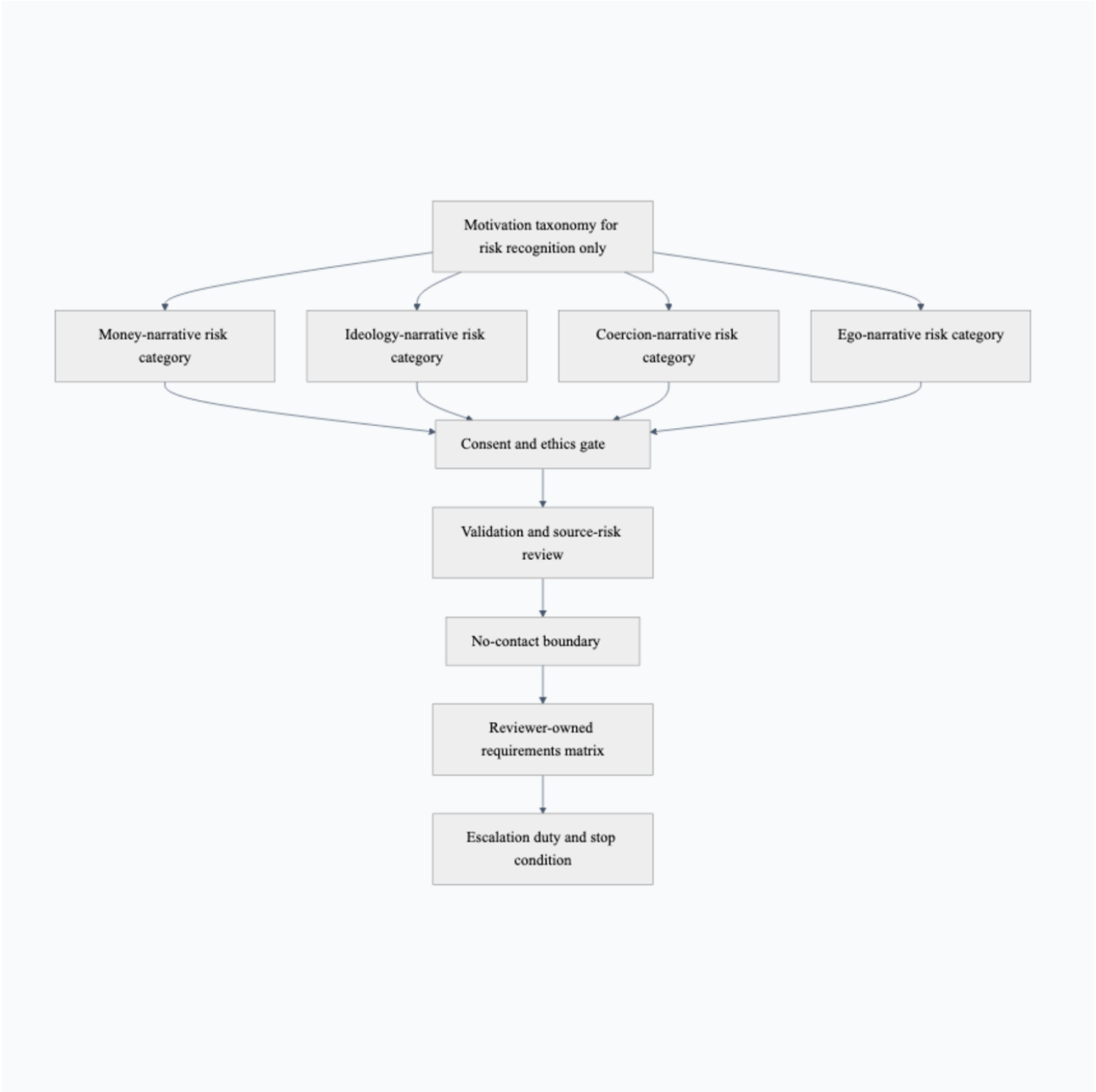


Figure 38: A study taxonomy for reading recruitment-risk literature as ethics, consent, and validation governance rather than as persuasion design. The captioned view belongs to the human intelligence humint / agent recruitment section and should be read as a map of Motivation taxonomy for risk recognition only, Money-narrative risk category, Ideology-narrative risk category, and Coercion-narrative risk category, not as a capability score or live-task instruction.

9.2 Requirements-to-Evidence Lens path for Agent Recruitment: lesson cluster, safe artifact, and review

Evidence anchor. Section 9; [238, 2026].

9.2.1 Agent Recruitment practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 9; [238, 2026].

9.2.2 Agent Recruitment topic lessons: source-backed concepts and transfer tasks

This module builds collection management as requirements discipline: a source method is considered only after the priority, authority, minimization rule, source risk, and evaluation plan are explicit. The sequence opens with **MICE Framework for recruitment-risk literacy**, **MICE Expanded: MICE Framework for recruitment-risk literacy**, **Spotting indicators literacy for recruitment-risk** and applies the **Requirements-to-Evidence Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 36; module overview Section 9; curriculum atlas Section 2.

Triangulation anchors. In module 4's topic-lessons section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

9.2.2.1 Lesson 1: MICE Framework for recruitment-risk literacy

Concept. MICE Framework for recruitment-risk literacy uses the motivation taxonomy to recognize recruitment-risk narratives and ethics constraints, not to design persuasion.

Why it matters. MICE Framework connects classroom vocabulary to Collection Management and Multi-INT Requirements Discipline practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. MICE Framework for recruitment-risk literacy rests on [020, 2026] and [021, 2026]. The most specific cited work observes: The article describes how the manuals cover intelligence methods such as agent recruitment, psychological manipulation, and disinformation detection, and notes the materials remain relevant because related methods persist in modern Russian services. Use them for fixing what **MICE Framework for recruitment-risk literacy** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. Read **MICE Framework** against the works cited for this row. [020, 2026] A publisher and training-organization page from HSM Training and Consultancy (London) promoting the book The Human Source Management System, a guide of over 500 pages that applies social psychology to the management of confidential informants. The site states the book draws on research and practitioner interviews and is used by law enforcement and intelligence bodies across more than 40 countries. [021, 2026] A July 2019 story from The World (PRX public radio) about a project led by Michael Weiss to translate previously unpublished Soviet-era KGB training manuals from the 1970s-80s into English. The article describes how the manuals cover intelligence methods such as agent recruitment, psychological manipulation, and disinformation detection, and notes the materials remain relevant because related methods persist in modern Russian services. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. Build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must note the motivation descriptor, the bounded claim about **MICE Framework**, the consent caveat, the uncertainty note, the no-contact boundary, and the reviewer who owns escalation duties. Shape this subject work as a **source-risk and validation ethics worksheet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **MICE Framework**: that a motivation taxonomy is a recruitment checklist.

Transfer task. Transfer **MICE Framework** from this module to a second motif by preserving requirements decomposition and source-discipline fit, replacing action with audit, and naming the blocked use.

9.2.2.2 Lesson 2: MICE Expanded: MICE Framework for recruitment-risk literacy

Concept. MICE Expanded: MICE Framework for recruitment-risk literacy uses the motivation taxonomy to recognize recruitment-risk narratives and ethics constraints, not to design persuasion.

Why it matters. MICE Expanded connects classroom vocabulary to Collection Management and Multi-INT Requirements Discipline practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. MICE Expanded: MICE Framework for recruitment-risk literacy rests on [298, 2026] and [297, 2026]. The closest source to this row notes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for the working definition that **MICE Expanded: MICE Framework for recruitment-risk literacy** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. Read **MICE Expanded** against the works cited for this row. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **MICE Expanded**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must note the motivation descriptor, the bounded claim about **MICE Expanded**, the consent caveat, the uncertainty note, the no-contact boundary, and the reviewer who owns escalation duties. Shape **MICE Expanded** work as a **source-risk and validation ethics worksheet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **MICE Expanded**: that a motivation taxonomy is a recruitment checklist.

Transfer task. Apply this module's safe boundary for **MICE Expanded** to another artifact while keeping requirements decomposition and source-discipline fit and reviewer ownership explicit.

9.2.2.3 Lesson 3: Spotting indicators literacy for recruitment-risk

Concept. Spotting indicators literacy for recruitment-risk reads recruitment doctrine as risk literacy: pressure, consent, validation, and the line that blocks operational contact.

Why it matters. Without explicit treatment of **Spotting indicators literacy**, confusing motivation literacy with contact authorization undermines requirements decomposition and source-discipline fit review; the lesson builds the habit to separate collection discipline concepts from operational recruitment, interception, or tasking procedures.

Source support. Spotting indicators literacy for recruitment-risk rests on [020, 2026] and [021, 2026]. The lead source's own note reads: A July 2019 story from The World (PRX public radio) about a project led by Michael Weiss to translate previously unpublished Soviet-era KGB training manuals from the 1970s-80s into English. Use them for the claim that **Spotting indicators literacy for recruitment-risk** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. For **Spotting indicators literacy**, reason from the sources cited in this row. [020, 2026] A publisher and training-organization page from HSM Training and Consultancy (London) promoting the book The Human Source Management System, a guide of over 500 pages that applies social psychology to the management of confidential informants. The site states the book draws on research and practitioner interviews and is used by law enforcement and intelligence bodies across more than 40 countries. [021, 2026] A July 2019 story from The World (PRX public radio) about a project led by Michael Weiss to translate previously unpublished Soviet-era KGB training manuals from the 1970s-80s into English. The article describes how the manuals cover intelligence methods such as agent recruitment, psychological manipulation, and disinformation detection, and notes the materials remain relevant because related methods persist in modern Russian services. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. Build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must note the motivation descriptor, the bounded claim about **Spotting indicators literacy**, the consent caveat, the uncertainty note, the no-contact boundary, and the reviewer who owns escalation duties. Shape this subject work as a **source-risk and validation ethics worksheet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Spotting indicators literacy**: that motivation literacy is contact authorization.

Transfer task. Transfer **Spotting indicators literacy** from this module to a second motif by preserving requirements decomposition and source-discipline fit, replacing action with audit, and naming the blocked use.

9.2.2.4 Lesson 4: Assessment-and-development ethics literacy

Concept. Assessment-and-development ethics literacy reads recruitment doctrine as risk literacy: pressure, consent, validation, and the line that blocks operational contact.

Why it matters. Without explicit treatment of **Assessment-and-development ethics literacy**, confusing motivation literacy with contact authorization undermines requirements decomposition and source-discipline fit review; the lesson builds the habit to separate collection discipline concepts from operational recruitment, interception, or tasking procedures.

Source support. Assessment-and-development ethics literacy rests on [020, 2026] and [021, 2026]. Its anchor reference records: The article describes how the manuals cover intelligence methods such as agent recruitment, psychological manipulation, and disinformation detection, and notes the materials remain relevant because related methods persist in modern Russian services. Use them for pinning down the scope of **Assessment-and-development ethics literacy**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. For **Assessment-and-development ethics literacy**, work from the cited evidence behind this row. [020, 2026] A publisher and training-organization page from HSM Training and Consultancy (London) promoting the book The Human Source Management System, a guide of over 500 pages that applies social psychology to the management of confidential informants. The site states the book draws on research and practitioner interviews and is used by law enforcement and intelligence bodies across more than 40 countries. [021, 2026] A July 2019 story from The World (PRX public radio) about a project led by Michael Weiss to translate previously unpublished Soviet-era KGB training manuals from the 1970s-80s into English. The article describes how the manuals cover intelligence methods such as agent recruitment, psychological manipulation, and disinformation detection, and notes the materials remain relevant because related methods persist in modern Russian services. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. Build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must note the motivation descriptor, the bounded claim about **Assessment-and-development ethics literacy**, the consent caveat, the uncertainty note, the no-contact boundary, and the reviewer who owns escalation duties. Shape this subject work as a **source-risk and validation ethics worksheet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Assessment-and-development ethics literacy**: that motivation literacy is contact authorization.

Transfer task. Transfer **Assessment-and-development ethics literacy** from this module to a second motif by preserving requirements decomposition and source-discipline fit, replacing action with audit, and naming the blocked use.

9.2.2.5 Lesson 5: Recruitment-doctrine ethics and source-protection literacy

Concept. Recruitment-doctrine ethics and source-protection literacy reads recruitment doctrine as risk literacy: pressure, consent, validation, and the line that blocks operational contact.

Why it matters. Recruitment-doctrine ethics connects classroom vocabulary to Collection Management and Multi-INT Requirements Discipline practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Recruitment-doctrine ethics and source-protection literacy rests on [020, 2026]. The most specific cited work observes: A publisher and training-organization page from HSM Training and Consultancy (London) promoting the book The Human Source Management System, a guide of over 500 pages that applies social psychology to the management of confidential informants. Use it for the working definition that **Recruitment-doctrine ethics and source-protection literacy** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. Ground **Recruitment-doctrine ethics** in the evidence the row cites. [020, 2026] A publisher and training-organization page from HSM Training and Consultancy (London) promoting the book The Human Source Management System, a guide of over 500 pages that applies social psychology to the management of confidential informants. The site states the book draws on research and practitioner interviews and is used by law enforcement and intelligence bodies across more than 40 countries. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. Build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must note the motivation descriptor, the bounded claim about **Recruitment-doctrine ethics**, the consent caveat, the uncertainty note, the no-contact boundary, and the reviewer who owns escalation duties. Shape this subject work as a **source-risk and validation ethics worksheet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Recruitment-doctrine ethics**: that motivation literacy is contact authorization.

Transfer task. Reuse the **Recruitment-doctrine ethics** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

9.2.2.6 Lesson 6: Declassified psychological-pressure ethics

Concept. Declassified psychological-pressure ethics reads recruitment doctrine as risk literacy: pressure, consent, validation, and the line that blocks operational contact.

Why it matters. Analysts use **Declassified psychological-pressure ethics** to separate collection discipline concepts from operational recruitment, interception, or tasking procedures. A defensible treatment names the judgment it enables for requirements decomposition and source-discipline fit review, the proof limit that opportunistic collection would otherwise hide, and the reviewer accountable for challenge.

Source support. Declassified psychological-pressure ethics rests on [021, 2026] and [022, 2026]. The closest source to this row notes: It summarizes a set of newly obtained manuals spanning several decades and describes the topics they cover, including operational terminology, agent classification, information-gathering methods, recruitment and vetting procedures, and counterintelligence concerns. Use them for the claim that **Declassified psychological-pressure ethics** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. For **Declassified psychological-pressure ethics**, work from the cited evidence behind this row. [021, 2026] A July 2019 story from The World (PRX public radio) about a project led by Michael Weiss to translate previously unpublished Soviet-era KGB training manuals from the 1970s-80s into English. The article describes how the manuals cover intelligence methods such as agent recruitment, psychological

manipulation, and disinformation detection, and notes the materials remain relevant because related methods persist in modern Russian services. [022, 2026] An article from The Interpreter, a publication focused on Russian affairs and disinformation, announcing a project to translate, analyze, and publish previously unpublished Soviet KGB training documents. It summarizes a set of newly obtained manuals spanning several decades and describes the topics they cover, including operational terminology, agent classification, information-gathering methods, recruitment and vetting procedures, and counterintelligence concerns. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. Build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must cite the declassified source descriptor, the bounded lesson about **Declassified psychological-pressure ethics**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape this subject work as a **source-risk and validation ethics worksheet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Declassified psychological-pressure ethics**: that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Apply this module's safe boundary for **Declassified psychological-pressure ethics** to another artifact while keeping requirements decomposition and source-discipline fit and reviewer ownership explicit.

9.2.2.7 Lesson 7: Digital-age recruitment-risk and consent-boundary Concept. Digital-age recruitment-risk and consent-boundary

Digital-age recruitment-risk and consent-boundary reads recruitment doctrine as risk literacy: pressure, consent, validation, and the line that blocks operational contact.

Why it matters. Analysts use **Digital-age recruitment-risk** to separate collection discipline concepts from operational recruitment, interception, or tasking procedures. A defensible treatment names the judgment it enables for requirements decomposition and source-discipline fit review, the proof limit that confusing motivation literacy with contact authorization would otherwise hide, and the reviewer accountable for challenge.

Source support. Digital-age recruitment-risk and consent-boundary rests on [023, 2026]. The lead source's own note reads: A 2024 International Master in Security, Intelligence and Strategic Studies thesis (Glasgow, Trento, Charles University) titled 'Human Intelligence in the Modern Era: The Impact of Digital Technology on Clandestine the module.' It uses a literature-based analysis plus three case studies to compare traditional human-source practices with technology-enabled approaches. Use it for pinning down the scope of **Digital-age recruitment-risk and consent-boundary**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. Read **Digital-age recruitment-risk** against the works cited for this row. [023, 2026] A 2024 International Master in Security, Intelligence and Strategic Studies thesis (Glasgow, Trento, Charles University) titled 'Human Intelligence in the Modern Era: The Impact of Digital Technology on Clandestine the module.' It uses a literature-based analysis plus three case studies to compare traditional human-source practices with technology-enabled approaches. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. Build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must note the motivation descriptor, the bounded claim about **Digital-age recruitment-risk**, the consent caveat, the uncertainty note, the no-contact boundary, and the reviewer who owns escalation duties. Shape this subject work as a **source-risk and validation ethics worksheet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Digital-age recruitment-risk**: that motivation literacy is contact authorization.

Transfer task. Transfer **Digital-age recruitment-risk** from this module to a second motif by preserving requirements decomposition and source-discipline fit, replacing action with audit, and naming the blocked use.

9.2.2.8 Lesson 8: Shared Experience as a Recruitment Tool: Experimental Research Concept. Shared Experience as a Recruitment Tool: Experimental Research

Shared Experience as a Recruitment Tool: Experimental Research reads recruitment doctrine as risk literacy: pressure, consent, validation, and the line that blocks operational contact.

Why it matters. Shared Experience as a Recruitment Tool connects classroom vocabulary to Collection Management and Multi-INT Requirements Discipline practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Shared Experience as a Recruitment Tool: Experimental Research rests on [024, 2026]. Use it for pinning down the scope of **Shared Experience as a Recruitment Tool: Experimental Research**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. For **Shared Experience as a Recruitment Tool**, reason from the sources cited in this row. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Shared Experience as a Recruitment Tool**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must note the motivation descriptor, the bounded claim about **Shared Experience as a Recruitment**, the consent caveat, the uncertainty note, the no-contact boundary, and the reviewer who owns escalation duties. Shape **Shared Experience as a Recruitment Tool** work as a **source-risk and validation ethics worksheet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Shared Experience as a Recruitment Tool**: that motivation literacy is contact authorization.

Transfer task. Transfer **Shared Experience as a Recruitment Tool** from this module to a second motif by preserving requirements decomposition and source-discipline fit, replacing action with audit, and naming the blocked use.

9.2.2.9 Lesson 9: How AI Lowers the Cost of Recruitment and Social Engineering Concept. How AI Lowers the Cost of Recruitment and Social Engineering

How AI Lowers the Cost of Recruitment and Social Engineering reads recruitment doctrine as risk literacy: pressure, consent, validation, and the line that blocks operational contact.

Why it matters. How AI Lowers the Cost matters in the **Collection Management and Multi-INT Requirements Discipline** lane because requirements decomposition and source-discipline fit evidence must stay separate from judgment; confusing motivation literacy with contact authorization is a common failure.

Source support. How AI Lowers the Cost of Recruitment and Social Engineering rests on [004, 2026]. The most specific cited work observes: He maintains that uniquely human qualities such as intuition, experience, and independent judgment become more valuable as adversaries gain access to the same AI tools. Use it for the claim that **How AI Lowers the Cost of Recruitment and Social Engineering** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. For **How AI Lowers the Cost**, reason from the sources cited in this row. [004, 2026] Tom Mulligan argues that artificial intelligence will enhance rather than replace human intelligence professionals, contending that the future of intelligence lies in human-machine collaboration. He maintains that uniquely human qualities such as intuition, experience, and independent judgment become more valuable as adversaries gain access to the same AI tools. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **How AI Lowers the Cost**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must note the motivation descriptor, the bounded claim about **How AI**

Lowers the Cost, the consent caveat, the uncertainty note, the no-contact boundary, and the reviewer who owns escalation duties. Shape **How AI Lowers the Cost** work as a **source-risk and validation ethics worksheet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **How AI Lowers the Cost**: that motivation literacy is contact authorization.

Transfer task. Transfer **How AI Lowers the Cost** from this module to a second motif by preserving requirements decomposition and source-discipline fit, replacing action with audit, and naming the blocked use.

9.2.2.10 Lesson 10: Recruitment Ethics and Legal Constraints **Concept. Recruitment Ethics and Legal Constraints** reads recruitment doctrine as risk literacy: pressure, consent, validation, and the line that blocks operational contact.

Why it matters. Recruitment Ethics matters in the **Collection Management and Multi-INT Requirements Discipline** lane because requirements decomposition and source-discipline fit evidence must stay separate from judgment; confusing motivation literacy with contact authorization is a common failure.

Source support. Recruitment Ethics and Legal Constraints rests on [298, 2026] and [297, 2026]. Its anchor reference records: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for pinning down the scope of **Recruitment Ethics and Legal Constraints**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. For **Recruitment Ethics**, work from the cited evidence behind this row. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. Build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must note the motivation descriptor, the bounded claim about **Recruitment Ethics**, the consent caveat, the uncertainty note, the no-contact boundary, and the reviewer who owns escalation duties. Shape this subject work as a **source-risk and validation ethics worksheet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Recruitment Ethics**: that motivation literacy is contact authorization.

Transfer task. Reuse the **Recruitment Ethics** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

9.2.3 Agent Recruitment worked safe example: synthetic inputs, evidence, and review

Worked example: a synthetic policy cell compares public indicators of hybrid pressure against an approved collection plan for a benign border-disruption exercise. [238, 2026]; [239, 2026].

Triangulation anchors. In module 4's worked-example section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **human-source literacy and source protection**. Learners use a **source-risk and validation ethics worksheet** and keep this boundary visible: No elicitation, impersonation, covert contact, or operational source-management procedures; all cases use classroom fixtures.

Frame. The classroom question centers on **MICE Framework for recruitment-risk literacy**. Excluded actions stay explicit, and the **Requirements-to-Evidence Lens** planning question is: What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit?

Inputs. For the **MICE Framework for recruitment-risk literacy** scenario, use public notices, synthetic interview summaries, public logistics records, and an instructor scope card. The Requirements-to-Evidence Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **MICE Framework for recruitment-risk literacy**, students rank requirements, choose the least intrusive source discipline, list excluded actions, and evaluate evidence quality. Pause whenever an inference about MICE Framework for recruitment-risk literacy appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **MICE Framework for recruitment-risk literacy** classroom scenario; unit artifact = source-risk and validation ethics worksheet; evidence = allowed inputs; method = requirements decomposition and source-discipline fit; output = a requirements-to-evidence matrix with discipline fit, source caveats, minimization notes, and gaps; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **MICE Framework for recruitment-risk literacy** as "Requirements-to-Evidence Lens confirms it" is not enough. The revision ties the claim to requirements decomposition and source-discipline fit, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **MICE Framework for recruitment-risk literacy** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

9.2.4 Agent Recruitment practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Requirements-to-Evidence Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**.

Triangulation anchors. In module 4's practice-sequence section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare MICE Framework for recruitment-risk literacy, MICE Expanded: MICE Framework for recruitment-risk literacy, Spotting indicators literacy for recruitment-risk; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Collection Management and Multi-INT Requirements Discipline** lane.

Move	Learner action	Output	Check
2. Frame	Answer the lens question: What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for MICE Framework for recruitment-risk literacy: requirements matrix with source descriptors, caveats, and collection limits.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the source-risk and validation ethics worksheet fields for MICE Framework for recruitment-risk literacy.	Unit profile note.	Evidence artifacts include validation note, pressure-risk checklist.
4. Challenge	Test the misconception that a motivation taxonomy is a recruitment checklist.	Failure-mode note.	The artifact applies the key distinction: separate collection discipline concepts from operational recruitment, interception, or tasking procedures.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

9.2.4.1 Agent Recruitment instructor notes: source reasoning, review points, and studio focus Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**. [238, 2026]; [239, 2026].

9.2.4.2 Agent Recruitment extension exercise: peer validation and refresh trigger review **Evidence anchor.** Section 9; [238, 2026]. Have learners swap artifacts and apply the **Requirements-to-Evidence Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**.

9.2.5 Agent Recruitment knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 9; [238, 2026].

1. Explain how **MICE Framework for recruitment-risk literacy** is defined here; name the source descriptor that supports the definition.
2. Contrast **MICE Framework for recruitment-risk literacy** with **MICE Expanded: MICE Framework for recruitment-risk literacy** using the **Requirements-to-Evidence Lens** artifact fields.
3. Identify one failure mode from the **Collection Management and Multi-INT Requirements Discipline** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which gray-zone indicator changes the least-intrusive source choice without crossing into operational tasking?
5. Correct this misconception: that a motivation taxonomy is a recruitment checklist.

9.2.5.1 Agent Recruitment answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **MICE Framework for recruitment-risk literacy** without source evidence, uncertainty, or a safe transfer task.

9.3 Agent Recruitment assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 9; [238, 2026].

9.3.1 Agent Recruitment evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 9; [238, 2026].

9.3.2 Agent Recruitment transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 9; [238, 2026].

9.3.2.1 Agent Recruitment lineage and source tradition: profile, concepts, and first anchors This sits in the **Collection Management and Multi-INT Requirements Discipline** lineage: requirements-driven, authority-bounded collection where priorities, legal basis, minimization, source protection, and evaluation are explicit. [238, 2026]; [239, 2026].

9.3.2.2 Agent Recruitment working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 9; [238, 2026].
The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**, with provenance and reviewability throughout.

9.3.2.3 Agent Recruitment knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** accountable requirements, source-discipline choices, minimization rules, source-risk notes, and evaluation criteria. [238, 2026]; [239, 2026].
- **Transforms:** priority mapping, source-discipline fit, least-intrusive evidence selection, and feedback review.
- **Outputs:** requirements matrix, collection-limit note, source-quality card, and gap list.
- **Failure modes:** recruitment or interception drift, over-collection, weak minimization, and source exposure.

9.3.2.4 Agent Recruitment transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 9; [238, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**.
- **Evidence contract:** keep the **Collection Management and Multi-INT Requirements Discipline** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as requirements matrix, collection-limit note, source-quality card, and gap list that another reviewer can audit.

9.3.2.5 Agent Recruitment profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 9; [238, 2026].
The matched profile emphasizes requirements-driven, authority-bounded collection where priorities, legal basis, minimization, source protection, and evaluation are explicit. The method stack is priority mapping, requirement decomposition, source-discipline fit, coverage-gap review, legal-authority check, and collection-feedback loop; the local topic cluster is **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**.

9.3.3 Agent Recruitment evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 9; [238, 2026].
Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Collection Management and Multi-INT Requirements Discipline** profile tells reviewers what evidence is strong enough for the module artifact built around **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**.

9.3.3.1 Agent Recruitment guide source spine: inherited keys and local citation roles Primary guide citations: [238, 2026]; [239, 2026]; [240, 2026]; [280, 2026]; [281, 2026]; [282, 2026]; [292, 2026]; [295, 2026]; [296, 2026]; [020, 2026]; [021, 2026]; [298, 2026]; [297, 2026]; [022, 2026]; [023, 2026]; [024, 2026]; [004, 2026].

9.3.3.2 Agent Recruitment verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [238, 2026]; [239, 2026].

Tier	What counts	How it is used
Source guide	[238, 2026]; [239, 2026]; [240, 2026]; [280, 2026]; [281, 2026]; [282, 2026]; [292, 2026]; [295, 2026]; [296, 2026]; [020, 2026]; [021, 2026]; [298, 2026]; [297, 2026]; [022, 2026]; [023, 2026]; [024, 2026]; [004, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 4's source-canon section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Maintenance rule: Perplexity may suggest candidates for **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy** and [238, 2026]; [239, 2026], but only directly verified source URLs are encoded as citations.

9.3.3.3 Agent Recruitment intelligence practice lens: evidence artifact and safety check Practice lens: **Requirements-to-Evidence Lens** for **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**. [238, 2026]; [239, 2026].

Planning question: What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit?

Evidence artifact: requirements matrix with source descriptors, caveats, and collection limits.

Validation rule: show priority, authority, minimization, corroboration, and source quality before any claim is reused. Applied to **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**.

Handoff contract: deliver metadata-rich evidence packets, not unscoped data piles or implicit targeting requests.

Safety check: exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure.

9.3.3.4 Agent Recruitment runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 9; [238, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	4.99	4.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Agent Recruitment to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Bounded autonomy, procurement, incident-response, and assurance studio	4.101	4.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Agent Recruitment	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Model-card, recoverability, retention, and learner-support evidence package	4.102	4.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Agent Recruitment	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
MICE Framework for recruitment-risk literacy	4.1	4.1 source title transformed into safe curriculum treatment; original: The MICE Framework: Money, Ideology, Coercion/Compromise, Ego	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
MICE Framework for recruitment-risk literacy	4.2	4.2 source title transformed into safe curriculum treatment; original: MICE Expanded: RASCLS — Reciprocity, Authority, Scarcity, Commitment, Liking, Social Proof	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Spotting indicators literacy for recruitment-risk	4.3	4.3 source title transformed into safe curriculum treatment; original: Targeting, Spotting, and Initial Assessment	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Assessment-and-development ethics literacy	4.4	4.4 source title transformed into safe curriculum treatment; original: Assessment and Development Operations	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Recruitment-doctrine ethics and source-protection literacy	4.5	4.5 source title transformed into safe curriculum treatment; original: The Recruitment Pitch: Methods and Psychology	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Declassified psychological-pressure ethics	4.6	4.6 source title transformed into safe curriculum treatment; original: KGB Recruitment Doctrine: Psychological Methods and Manipulation	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Digital-age recruitment-risk and consent-boundary	4.7	4.7 source title transformed into safe curriculum treatment; original: Digital-Age Recruitment: LinkedIn, Telegram, Cryptocurrencies, Dark Web	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Shared Experience as a Recruitment Tool: Experimental Research	4.8	4.8 Shared Experience as a Recruitment Tool: Experimental Research	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
How AI Lowers the Cost of Recruitment and Social Engineering	4.9	4.9 How AI Lowers the Cost of Recruitment and Social Engineering	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Recruitment Ethics and Legal Constraints	4.10	4.10 Recruitment Ethics and Legal Constraints	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

9.3.3.5 Agent Recruitment reusable subsection contract: topic rows, artifacts, and safety duties **Evidence anchor.** Section 9; [238, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
MICE Framework for recruitment-risk literacy	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
MICE Expanded: MICE Framework for recruitment-risk literacy	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Spotting indicators literacy for recruitment-risk	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

Lesson topic	Practice lens	Evidence artifact	Safety check
Assessment-and-development ethics literacy	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Recruitment-doctrine ethics and source-protection literacy	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Declassified psychological-pressure ethics	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Digital-age recruitment-risk and consent-boundary	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Shared Experience as a Recruitment Tool: Experimental Research	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
How AI Lowers the Cost of Recruitment and Social Engineering	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Recruitment Ethics and Legal Constraints	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

9.3.3.6 Agent Recruitment annotated source ledger: real titles and local contribution Each source cited by this **Collection Management and Multi-INT Requirements Discipline** module is paired below with its real title and a one-line note on what it contributes to **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**.

Source	Cited work	What it contributes	Status
[238, 2026]	Recommendation on the Ethics of Artificial Intelligence	The official UNESCO page for the Recommendation on the Ethics of Artificial Intelligence, the first global standard-setting instrument on AI ethics, adopted in 2021 and applicable to all 194 member states. It outlines four core values, including human rights protection and environmental flourishing, and ten guiding principles such as proportionality, privacy, transparency, and fairness.	verified source-guide
[239, 2026]	Digital Space and Human Rights	Official OHCHR digital rights portal.	original source-guide
[240, 2026]	The Right to Privacy in the Digital Age	The Office of the High Commissioner for Human Rights (OHCHR) hub page on the right to privacy in the digital age. It addresses how data-intensive technologies, particularly artificial intelligence, create risks for privacy, autonomy, and human dignity, and curates international standards, reports, and expert consultations.	verified source-guide
[280, 2026]	NIST SP 800-61 Rev. 3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management	NIST SP 800-61 Rev. 3, published April 2025, integrates incident response guidance into broader cybersecurity risk management aligned with the NIST Cybersecurity Framework 2.0, superseding the 2012 Rev. 2. The publication addresses cyber threat information sharing, incident handling and management practices, and procedures for detecting, responding to, and recovering from security incidents.	verified source-guide

Source	Cited work	What it contributes	Status
[281, 2026]	Artificial Intelligence Cybersecurity Challenges	An ENISA (European Union Agency for Cybersecurity) report published December 15, 2020 mapping the cybersecurity challenges of artificial intelligence. It defines AI scope through a lifecycle approach, identifies the assets requiring protection within AI ecosystems, and develops a threat taxonomy classified across lifecycle stages and asset categories.	verified source-guide
[282, 2026]	AI Research: Security and Resilience	A NIST page on AI research focused on security and resilience, framing these as core characteristics of trustworthy AI under the NIST AI Risk Management Framework.	verified source-guide
[292, 2026]	Assessing Risks and Impacts of AI (ARIA): Pilot Evaluation Report	The ARIA 0.1 pilot evaluation report documents NIST's methodology for systematically assessing AI applications for risks and societal impacts, using a multi-layered evaluation approach across five participating organizations and seven submitted AI applications. The pilot employed three evaluation scenarios and three testing levels: model testing, red teaming, and field testing, supplemented by dialogue annotation, tester questionnaires, and structured measurement trees.	verified source-guide
[295, 2026]	M-25-22: Driving Efficient Acquisition of Artificial Intelligence in Government	OMB Memorandum M-25-22 (April 3, 2025), Driving Efficient Acquisition of Artificial Intelligence in Government, issued under Executive Order 13960 and related directives. It provides guidance to federal agencies for acquiring effective and trustworthy AI in a timely, cost-effective manner, and rescinds and replaces earlier memorandum M-24-18.	verified source-guide
[296, 2026]	Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile	NIST AI 600-1, the Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, a cross-sectoral companion resource to the NIST AI RMF 1.0 issued pursuant to Executive Order 14110. It identifies risks that are unique to or amplified by generative AI and organizes suggested actions for managing those risks, mapped to the AI RMF functions.	verified source-guide
[020, 2026]	The Human Source Management System (Confidential Informant	A publisher and training-organization page from HSM Training and Consultancy (London) promoting the book The Human Source Management System, a guide of over 500 pages that applies social psychology to the management of confidential informants. The site states the book draws on research and practitioner interviews and is used by law enforcement and intelligence bodies across more than 40 countries.	verified source-guide

Source	Cited work	What it contributes	Status
[021, 2026]	Learn how to be a spy from previously unpublished KGB training	A July 2019 story from The World (PRX public radio) about a project led by Michael Weiss to translate previously unpublished Soviet-era KGB training manuals from the 1970s-80s into English. The article describes how the manuals cover intelligence methods such as agent recruitment, psychological manipulation, and disinformation detection, and notes the materials remain relevant because related methods persist in modern Russian services.	verified source-guide
[298, 2026]	Intelligence Community Directives	Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations.	original source-guide
[297, 2026]	Intelligence Community Directive 203: Analytic Standards	Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products.	original source-guide
[022, 2026]	Summaries of Newly Obtained KGB Training Manuals - The Interpreter	An article from The Interpreter, a publication focused on Russian affairs and disinformation, announcing a project to translate, analyze, and publish previously unpublished Soviet KGB training documents. It summarizes a set of newly obtained manuals spanning several decades and describes the topics they cover, including operational terminology, agent classification, information-gathering methods, recruitment and vetting procedures, and counterintelligence concerns.	verified source-guide
[023, 2026]	The Impact of Digital Technology on Clandestine Agent Recruitment	A 2024 International Master in Security, Intelligence and Strategic Studies thesis (Glasgow, Trento, Charles University) titled 'Human Intelligence in the Modern Era: The Impact of Digital Technology on Clandestine Agent Recruitment.' It uses a literature-based analysis plus three case studies to compare traditional human-source practices with technology-enabled approaches.	verified source-guide
[024, 2026]	Using shared experiences to recruit committed human intelligence	See bibliography for scope.	original source-guide
[004, 2026]	AI Won't Replace Spies—It Will Make Them More Powerful Than Ever	Tom Mulligan argues that artificial intelligence will enhance rather than replace human intelligence professionals, contending that the future of intelligence lies in human-machine collaboration. He maintains that uniquely human qualities such as intuition, experience, and independent judgment become more valuable as adversaries gain access to the same AI tools.	verified source-guide

Where this sits. This module's overview is Section 9; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

9.3.4 Agent Recruitment governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 9; [238, 2026].

9.3.5 Agent Recruitment analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 4's governance-boundary section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **Collection Management and Multi-INT Requirements Discipline** for **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**. [238, 2026]; [239, 2026].

Curriculum topic spine: MICE Framework for recruitment-risk literacy, **MICE Expanded: MICE Framework for recruitment-risk literacy**, **Spotting indicators literacy for recruitment-risk**. **Verified anchor cluster:** [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]; [Archives and Administration, 1981]; [Agency, 2026g]; [of the Director of National Intelligence, 2026d].

Conceptual depth: requirements-driven, authority-bounded collection where priorities, legal basis, minimization, source protection, and evaluation are explicit.

Method stack: priority mapping, requirement decomposition, source-discipline fit, coverage-gap review, legal-authority check, and collection-feedback loop.

Composability contract: requirements, authorities, source disciplines, collection notes, retention limits, caveats, and evaluation metrics remain separable.

Known failure modes: opportunistic collection, priority drift, over-collection, weak minimization, source exposure, and confusing availability with authority.

Defensive boundary: collection material remains doctrinal and governance-oriented; it does not teach recruitment, interception, surveillance, or tasking procedures. Applied to **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**.

Anchor	Why it matters here
[Community, 2026]	Official public explanation of the intelligence cycle, collection disciplines, dissemination, evaluation, oversight, and partners. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026c]	Official prioritization directive for translating national intelligence priorities into collection, analysis, risk management, and responsiveness evaluation. Checked as of 2026-05-21; role: curriculum_anchor.
[of Staff, 2026]	Official joint-doctrine landing page for the keystone publication on joint intelligence principles, products, services, and assessments. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence and Agency, 2024]	Official IC OSINT strategy for professionalizing OSINT, integrated collection management, open-source sharing, innovation, and tradecraft. Checked as of 2026-05-21; role: curriculum_anchor.
[Archives and Administration, 1981]	Official legal anchor for intelligence authorities, rights-aware collection, analytic competition, oversight, and source-method protection. Checked as of 2026-05-21; role: curriculum_anchor.
[Agency, 2026g]	Official NSA public explanation of FISA oversight for signals intelligence collection governed by statutory and court-authorized controls. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026d]	Official sourcing directive for traceability, citations, source descriptors, and source summaries. Checked as of 2026-05-21; role: curriculum_anchor.

9.3.5.1 Agent Recruitment evidence standard and citation floor: source families and discovery limits Official guidance supplies governance, safety, and legal constraints for the **Collection Management and Multi-INT Requirements Discipline** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [238, 2026]; [239, 2026].

9.3.6 Agent Recruitment agentic boundary: assist, approve, block, and record

Evidence anchor. Section 9; [238, 2026].

AGEINT translation is bounded by the **Collection Management and Multi-INT Requirements Discipline** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**.

9.3.6.1 Agent Recruitment permitted defensive utility: curriculum uses and safe outputs **Evidence anchor.** Section 9; [238, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**.

9.3.6.2 Agent Recruitment excluded operational boundary: blocked actions and stop rules Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [238, 2026]; [239, 2026] and **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

9.3.7 Agent Recruitment governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 9; [238, 2026].

Governance is practiced as a gate on the **Collection Management and Multi-INT Requirements Discipline** lane. Learners use the **Requirements-to-Evidence Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues

remain, and when an agent-assisted artifact must stop for human review while using **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**.

9.3.7.1 Agent Recruitment governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [238, 2026]; [239, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Collection Management and Multi-INT Requirements Discipline** failure modes and the **Requirements-to-Evidence Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

9.3.7.2 Agent Recruitment evidence package handoff: appendices, records, and reuse

Evidence anchor. Section 9; [238, 2026]. Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Requirements-to-Evidence Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**.

9.3.7.3 Agent Recruitment current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**. [238, 2026]; [239, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_intelligence_gov_how_ic_works` for **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**?	How the IC Works; lane `governed_intelligence_cycle`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official public explanation of the intelligence cycle, collection disciplines, dissemination, evaluation, oversight, and partners.
What does the module inherit from `official_odni_icd_204` for **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**?	Intelligence Community Directive 204: National Intelligence Priorities Framework; lane `collection_management`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official prioritization directive for translating national intelligence priorities into collection, analysis, risk management, and responsiveness evaluation.
What does the module inherit from `official_joint_pub_2_0` for **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**?	JP 2-0: Joint Intelligence; lane `collection_management`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official joint-doctrine landing page for the keystone publication on joint intelligence principles, products, services, and assessments.
What does the module inherit from `official_ic_osint_strategy` for **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**?	The INT of First Resort: The IC OSINT Strategy 2024-2026; lane `osint_geoint`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official IC OSINT strategy for professionalizing OSINT, integrated collection management, open-source sharing, innovation, and tradecraft.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 9; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

9.3.8 Agent Recruitment assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 9; [238, 2026].

9.3.9 Agent Recruitment assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 9; [238, 2026].

9.3.9.1 Agent Recruitment capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy** and [238, 2026]; [239, 2026].

9.3.9.2 Agent Recruitment instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy** and [238, 2026]; [239, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

9.3.9.3 Agent Recruitment assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
MICE Framework for recruitment-risk literacy	Completed **requirements matrix with source descriptors, caveats, and collection limits** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
MICE Expanded: MICE Framework for recruitment-risk literacy	Completed **requirements matrix with source descriptors, caveats, and collection limits** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Spotting indicators literacy for recruitment-risk	Completed **requirements matrix with source descriptors, caveats, and collection limits** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

9.3.10 Agent Recruitment refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [238, 2026]; [239, 2026] and **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**.

9.3.10.1 Agent Recruitment refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**. The local signals begin with [238, 2026]; [239, 2026].

9.3.10.2 Agent Recruitment claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**, and the source spine for these checks begins with [238, 2026]; [239, 2026].

9.3.11 Agent Recruitment reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [238, 2026]; [239, 2026].

Triangulation anchors. In module 4's review-checklist section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy**. [238, 2026]; [239, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

9.3.12 Agent Recruitment learning-path links: module map, overview, and curriculum atlas

Follow the cross-links to move between **MICE Framework for recruitment-risk literacy; MICE Expanded: MICE Framework for recruitment-risk literacy** and the rest of the curriculum without losing the source spine: orientation first, then the parent unit, then the modules on either side. Primary sources: [238, 2026]; [239, 2026].

Section 2, Section 8, Section 10

10 Agent Handling and Management

10.0.1 Agent Handling and Management figures and course links: visual evidence, source flow, and navigation

The module uses Figure 39 and Figure 36 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 8, Section 9, Section 11.
This module teaches the **Collection Management and Multi-INT Requirements Discipline** lane through a bounded, source-backed coursebook chapter. [239, 2026]; [240, 2026].

10.1 Collection Management and Multi-INT Requirements Discipline frame for Agent Handling and Management: source context, topic focus, and reader task

Evidence anchor. Section 10; [239, 2026].

10.1.1 Agent Handling and Management orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 10; [239, 2026].

10.1.2 Agent Handling and Management conceptual primer: source context, core model, and reader task

This chapter teaches collection management as requirements discipline: a source method is considered only after the priority, authority, minimization rule, source risk, and evaluation plan are explicit. The chapter uses **Requirements-to-Evidence Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**.
The central distinction is to separate collection discipline concepts from operational recruitment, interception, or tasking procedures. Core topics include **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics; Historical surveillance-risk and source-protection**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [239, 2026]; [240, 2026].
Learners move from vocabulary and the **Requirements-to-Evidence Lens** distinction through topic lessons on **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust** with evidence and misconception checks, then assemble a **requirements matrix with source descriptors, caveats, and collection limits** with safety and rights gates.

10.1.3 Agent Handling and Management learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 10; [239, 2026].

- Connect **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust and Historical meeting-structure ethics** to **Collection Management and Multi-INT Requirements Discipline** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **requirements matrix with source descriptors, caveats, and collection limits** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate collection discipline concepts from operational recruitment, interception, or tasking procedures; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as opportunistic collection, priority drift, over-collection, weak minimization, source exposure, and confusing availability with authority, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: collection material remains doctrinal and governance-oriented; it does not teach recruitment, interception, surveillance, or tasking procedures.

10.1.4 Agent Handling and Management core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 10; [239, 2026].

Term	Working definition
Priority	the relative importance of an intelligence question
Source discipline	a broad evidence channel such as HUMINT, SIGINT, GEOINT, OSINT, or FININT
Minimization	the rule that limits acquisition, retention, or use of unnecessary information
Source protection	the duty to reduce risk to people, methods, and sensitive relationships
Evaluation	the feedback step that tests whether the evidence satisfied the requirement
Gray-zone indicator	an observable signal of ambiguous coercion below armed conflict thresholds
Proxy pattern	a relationship suggesting indirect sponsorship without confirmed operational control
The Case Officer–Agent Relationship: Building,...	Key terms: Case, Officer, Agent.
Historical meeting-structure ethics	Key terms: Historical, meeting, structure.

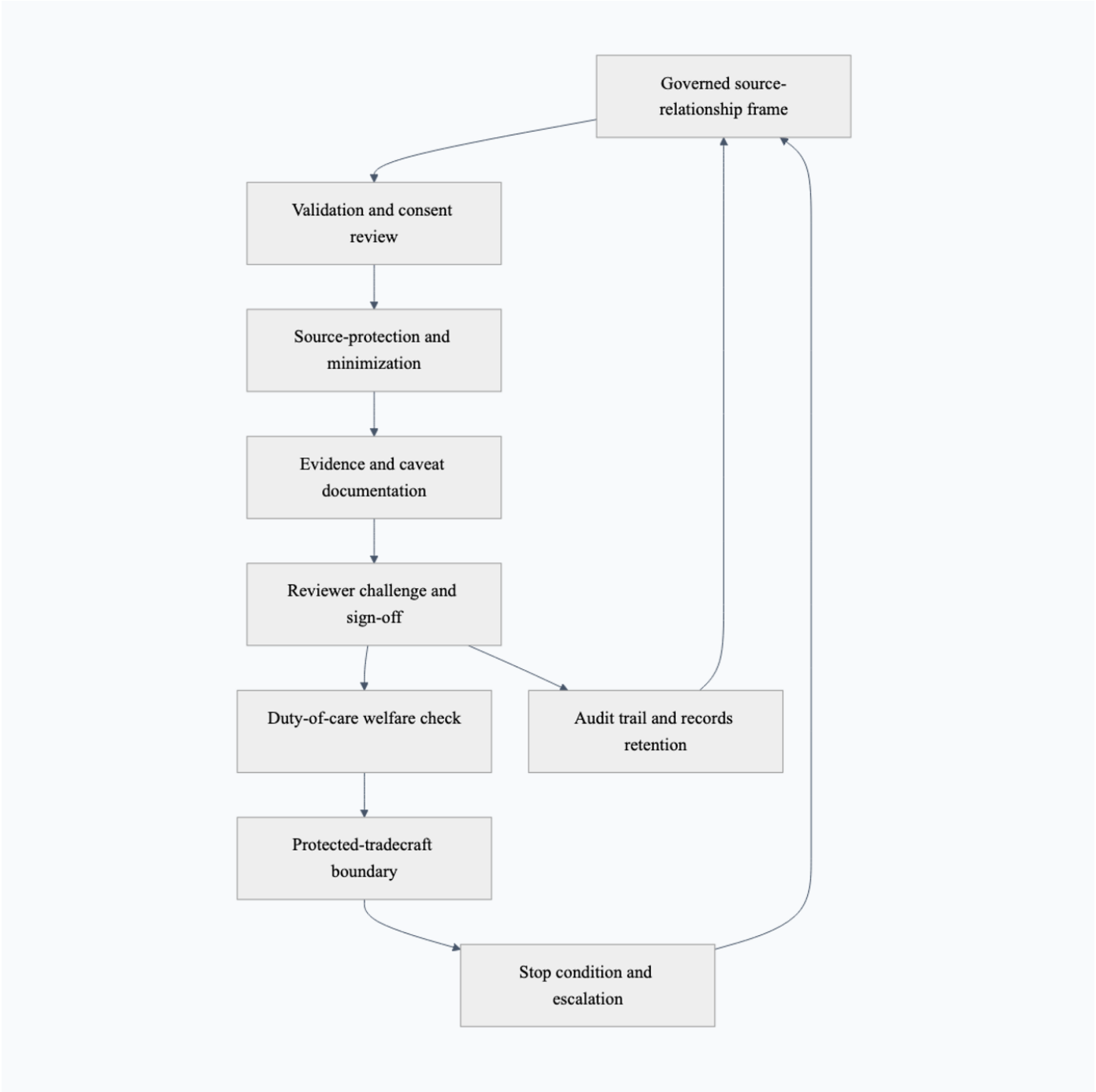


Figure 39: The governed review cycle for documenting source relationships, protection, and reviewer accountability without recreating handling procedures. In the human intelligence humint / agent handling and management section, it lets readers compare Governed source-relationship frame, Validation and consent review, Source-protection and minimization, and Evidence and caveat documentation so the visual functions as a traceable course aid rather than an unscoped assertion.

10.2 Requirements-to-Evidence Lens path for Agent Handling and Management: lesson cluster, safe artifact, and review

Evidence anchor. Section 10; [239, 2026].

10.2.1 Agent Handling and Management practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 10; [239, 2026].

10.2.2 Agent Handling and Management topic lessons: source-backed concepts and transfer tasks

This module builds collection management as requirements discipline: a source method is considered only after the priority, authority, minimization rule, source risk, and evaluation plan are explicit. The sequence opens with **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust**, **Historical meeting-structure ethics**, **Historical surveillance-risk and source-protection** and applies the **Requirements-to-Evidence Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 36; module overview Section 10; curriculum atlas Section 2.

Triangulation anchors. In module 5's topic-lessons section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

10.2.2.1 Lesson 1: The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust **Concept. The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust** treats human-source work as a governed relationship: validation, consent, reporting, source protection, and oversight—not contact activity.

Why it matters. Without explicit treatment of **The Case Officer–Agent Relationship**, opportunistic collection undermines requirements decomposition and source-discipline fit review; the lesson builds the habit to separate collection discipline concepts from operational recruitment, interception, or tasking procedures.

Source support. The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust rests on [025, 2026]. The closest source to this row notes: It also addresses how operatives are selected, the isolation of covert work, and its psychological effects on personal relationships. Use it for pinning down the scope of **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. Ground **The Case Officer–Agent Relationship** in the evidence the row cites. [025, 2026] This is an episode of The Unmistakable Creative Podcast featuring former CIA field operative Andrew Bustamante discussing intelligence work. The conversation covers his background at the Air Force Academy and CIA training, and frames espionage as resting on reading people, trust, influence, and empathy rather than glamour or action. It also addresses how operatives are selected, the isolation of covert work, and its psychological effects on personal relationships. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **The Case Officer–Agent Relationship**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must name the source descriptor, the bounded claim about **Case Officer Agent Relationship**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **The Case Officer–Agent Relationship** work as a **source-risk and validation ethics worksheet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust is optional whenever separate collection discipline concepts from operational recruitment, interception, or tasking procedures feels inconvenient.

Transfer task. Transfer **The Case Officer–Agent Relationship** to a second module by preserving requirements decomposition and source-discipline fit, changing the source evidence, and naming a new reviewer.

10.2.2.2 Lesson 2: Historical meeting-structure ethics **Concept. Historical meeting-structure ethics** uses the historical motif to discuss source-protection ethics, documentation, and oversight without recreating handling procedures.

Why it matters. Historical meeting-structure ethics matters in the **Collection Management and Multi-INT Requirements Discipline** lane because requirements decomposition and source-discipline fit evidence must stay separate from judgment; opportunistic collection is a common failure.

Source support. Historical meeting-structure ethics rests on [029, 2026] and [004, 2026]. The closest source to this row notes: It surveys the roles of case officers in managing sources, recruitment and training of agents, protective measures such as fronts and cutouts, agent classifications including unwitting sources, and counterintelligence methods for identifying foreign operatives and reducing security breaches. Use them for fixing what **Historical meeting-structure ethics** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. Ground **Historical meeting-structure ethics** in the evidence the row cites. [029, 2026] A roughly 28-page Scribd document titled "Agent Handling in Counterintelligence" providing an educational overview of intelligence operations. It surveys the roles of case officers in managing sources, recruitment and training of agents, protective measures such as fronts and cutouts, agent classifications including unwitting sources, and counterintelligence methods for identifying foreign operatives and reducing security breaches. [004, 2026] Tom Mulligan argues that artificial intelligence will enhance rather than replace human intelligence professionals, contending that the future of intelligence lies in human-machine collaboration. He maintains that uniquely human qualities such as intuition, experience, and independent judgment become more valuable as adversaries gain access to the same AI tools. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. Build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must cite the historical descriptor, the bounded lesson about **Historical meeting-structure ethics**, the handling caveat, the uncertainty note, the protected-tradecraft boundary, and the reviewer who clears the account. Shape this subject work as a **source-risk and validation ethics worksheet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Historical meeting-structure ethics**: that a documented handling precedent licenses repeating the approach, rather than a case-bound record whose risks must be re-assessed each time.

Transfer task. Reuse the **Historical meeting-structure ethics** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

10.2.2.3 Lesson 3: Historical surveillance-risk and source-protection **Concept. Historical surveillance-risk and source-protection** uses the historical motif to discuss source-protection ethics, documentation, and oversight without recreating handling procedures.

Why it matters. Historical surveillance-risk matters in the **Collection Management and Multi-INT Requirements Discipline** lane because requirements decomposition and source-discipline fit evidence must stay separate from judgment; opportunistic collection is a common failure.

Source support. Historical surveillance-risk and source-protection rests on [026, 2026] and [016, 2026]. The most specific cited work observes: It conveys the difficulty and stress of clandestine field meetings as recounted from personal experience. Use them for fixing what **Historical surveillance-risk and source-protection** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. Ground **Historical surveillance-risk** in the evidence the row cites. [026, 2026] A YouTube video titled "Inside the CIA: The tension and drama behind surveillance detection operations," released May 3, 2024, featuring a former CIA officer. The speaker describes the operational complexity and interpersonal tension involved in moving safely from a starting point to a meeting while accounting for the presence of hostile observation. It conveys the difficulty and stress of clandestine field meetings as recounted from personal experience. [016, 2026] Place where victim can be controlled with limited avenues of escape. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. Build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must cite the historical descriptor, the bounded lesson about **Historical surveillance-risk**, the handling caveat, the uncertainty note, the protected-tradecraft boundary, and the reviewer who clears the account. Shape this subject work as a **source-risk and validation ethics worksheet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Historical surveillance-risk**: that a documented handling precedent licenses repeating the approach, rather than a case-bound record whose risks must be re-assessed each time.

Transfer task. Transfer **Historical surveillance-risk** from this module to a second motif by preserving requirements decomposition and source-discipline fit, replacing action with audit, and naming the blocked use.

10.2.2.4 Lesson 4: Historical clandestine-communications ethics

Concept. Historical clandestine-communications ethics uses the historical motif to discuss source-protection ethics, documentation, and oversight without recreating handling procedures.

Why it matters. Without explicit treatment of **Historical clandestine-communications ethics**, opportunistic collection undermines requirements decomposition and source-discipline fit review; the lesson builds the habit to separate collection discipline concepts from operational recruitment, interception, or tasking procedures.

Source support. Historical clandestine-communications ethics rests on [027, 2026] and [028, 2026]. The most specific cited work observes: Learn a technique for communicating with your family in an emergency using a method used by spies. Use them for the claim that **Historical clandestine-communications ethics** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. For **Historical clandestine-communications ethics**, reason from the sources cited in this row. [027, 2026] Learn a technique for communicating with your family in an emergency using a method used by spies. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. Build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must cite the historical descriptor, the bounded lesson about **Historical clandestine-communications ethics**, the handling caveat, the uncertainty note, the protected-tradecraft boundary, and the reviewer who clears the account. Shape this subject work as a **source-risk and validation ethics worksheet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Historical clandestine-communications ethics**: that a documented handling precedent licenses repeating the approach, rather than a case-bound record whose risks must be re-assessed each time.

Transfer task. Apply this module's safe boundary for **Historical clandestine-communications ethics** to another artifact while keeping requirements decomposition and source-discipline fit and reviewer ownership explicit.

10.2.2.5 Lesson 5: Historical cutout-and-intermediary provenance

Concept. Historical cutout-and-intermediary provenance uses the historical motif to discuss source-protection ethics, documentation, and oversight without recreating handling procedures.

Why it matters. Analysts use **Historical cutout-and-intermediary provenance** to separate collection discipline concepts from operational recruitment, interception, or tasking procedures. A defensible treatment names the judgment it enables for requirements decomposition and source-discipline fit review, the proof limit that opportunistic collection would otherwise hide, and the reviewer accountable for challenge.

Source support. Historical cutout-and-intermediary provenance rests on [029, 2026]. The most specific cited work observes: It surveys the roles of case officers in managing sources, recruitment and training of agents, protective measures such as fronts and cutouts, agent classifications including unwitting sources, and counterintelligence methods for identifying foreign operatives and reducing security breaches. Use it for the claim that **Historical cutout-and-intermediary provenance** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. Ground **Historical cutout-and-intermediary provenance** in the evidence the row cites. [029, 2026] A roughly 28-page Scribd document titled "Agent Handling in Counterintelligence" providing an educational overview of intelligence operations. It surveys the roles of case officers in managing sources, recruitment and training of agents, protective measures such as fronts and cutouts, agent classifications including unwitting sources, and counterintelligence methods for identifying foreign operatives and reducing security breaches. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. Build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must cite the historical descriptor, the bounded lesson about **Historical cutout-and-intermediary provenance**, the handling caveat, the uncertainty note, the protected-tradecraft boundary, and the reviewer who clears the account. Shape this subject work as a **source-risk and validation ethics worksheet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Historical cutout-and-intermediary provenance**: that a documented handling precedent licenses repeating the approach, rather than a case-bound record whose risks must be re-assessed each time.

Transfer task. Transfer **Historical cutout-and-intermediary provenance** from this module to a second motif by preserving requirements decomposition and source-discipline fit, replacing action with audit, and naming the blocked use.

10.2.2.6 Lesson 6: Historical front-entity provenance

Concept. Historical front-entity provenance treats agents as software actors with explicit permissions, logs, stop conditions, and human approval—not autonomous decision makers.

Why it matters. Without explicit treatment of **Historical front-entity provenance**, opportunistic collection undermines requirements decomposition and source-discipline fit review; the lesson builds the habit to separate collection discipline concepts from operational recruitment, interception, or tasking procedures.

Source support. Historical front-entity provenance rests on [029, 2026]. The closest source to this row notes: A roughly 28-page Scribd document titled "Agent Handling in Counterintelligence" providing an educational overview of intelligence operations. Use it for pinning down the scope of **Historical front-entity provenance**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. Read **Historical front-entity provenance** against the works cited for this row. [029, 2026] A roughly 28-page Scribd document titled "Agent Handling in Counterintelligence" providing an educational overview of intelligence operations. It surveys the roles of case officers in managing sources, recruitment and training of agents, protective measures such as fronts and cutouts, agent classifications including unwitting

sources, and counterintelligence methods for identifying foreign operatives and reducing security breaches. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. Build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must cite the historical descriptor, the bounded lesson about **Historical front-entity provenance**, the handling caveat, the uncertainty note, the protected-tradecraft boundary, and the reviewer who clears the account. Shape this subject work as a **source-risk and validation ethics worksheet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Historical front-entity provenance**: that a documented handling precedent licenses repeating the approach, rather than a case-bound record whose risks must be re-assessed each time.

Transfer task. Apply this module's safe boundary for **Historical front-entity provenance** to another artifact while keeping requirements decomposition and source-discipline fit and reviewer ownership explicit.

10.2.2.7 Lesson 7: Counter-Surveillance and Detecting Hostile Surveillance: Historical surveillance-risk and source-protection

Concept. Counter-Surveillance and Detecting Hostile Surveillance: Historical surveillance-risk and source-protection uses the historical motif to discuss source-protection ethics, documentation, and oversight without recreating handling procedures.

Why it matters. Without explicit treatment of **Counter-Surveillance and Detecting Hostile Surveillance**, opportunistic collection undermines requirements decomposition and source-discipline fit review; the lesson builds the habit to separate collection discipline concepts from operational recruitment, interception, or tasking procedures.

Source support. Counter-Surveillance and Detecting Hostile Surveillance: Historical surveillance-risk and source-protection rests on [030, 2026] and [031, 2026]. The closest source to this row notes: There are cameras everywhere! Use them for the working definition that **Counter-Surveillance and Detecting Hostile Surveillance: Historical surveillance-risk and source-protection** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. For **Counter-Surveillance and Detecting Hostile Surveillance**, reason from the sources cited in this row. [031, 2026] There are cameras everywhere! Everything is trackable! Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Counter-Surveillance and Detecting Hostile Surveillance**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must cite the historical descriptor, the bounded lesson about **Counter-Surveillance and Detecting Hostile Surveillance**, the handling caveat, the uncertainty note, the protected-tradecraft boundary, and the reviewer who clears the account. Shape **Counter-Surveillance and Detecting Hostile Surveillance** work as a **source-risk and validation ethics worksheet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Counter-Surveillance and Detecting Hostile Surveillance**: that a documented handling precedent licenses repeating the approach, rather than a case-bound record whose risks must be re-assessed each time.

Transfer task. Reuse the **Counter-Surveillance and Detecting Hostile Surveillance** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

10.2.2.8 Lesson 8: Historical agent-tasking oversight

Concept. Historical agent-tasking oversight treats agents as software actors with explicit permissions, logs, stop conditions, and human approval—not autonomous decision makers.

Why it matters. Historical agent-tasking oversight connects classroom vocabulary to Collection Management and Multi-INT Requirements Discipline practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Historical agent-tasking oversight rests on [029, 2026] and [004, 2026]. Its anchor reference records: A roughly 28-page Scribd document titled "Agent Handling in Counterintelligence" providing an educational overview of intelligence operations. Use them for the claim that **Historical agent-tasking oversight** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. For **Historical agent-tasking oversight**, work from the cited evidence behind this row. [029, 2026] A roughly 28-page Scribd document titled "Agent Handling in Counterintelligence" providing an educational overview of intelligence operations. It surveys the roles of case officers in managing sources, recruitment and training of agents, protective measures such as fronts and cutouts, agent classifications including unwitting sources, and counterintelligence methods for identifying foreign operatives and reducing security breaches. [004, 2026] Tom Mulligan argues that artificial intelligence will enhance rather than replace human intelligence professionals, contending that the future of intelligence lies in human-machine collaboration. He maintains that uniquely human qualities such as intuition, experience, and independent judgment become more valuable as adversaries gain access to the same AI tools. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. Build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must cite the historical descriptor, the bounded lesson about **Historical agent-tasking oversight**, the handling caveat, the uncertainty note, the protected-tradecraft boundary, and the reviewer who clears the account. Shape this subject work as a **source-risk and validation ethics worksheet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Historical agent-tasking oversight**: that a documented handling precedent licenses repeating the approach, rather than a case-bound record whose risks must be re-assessed each time.

Transfer task. Transfer **Historical agent-tasking oversight** from this module to a second motif by preserving requirements decomposition and source-discipline fit, replacing action with audit, and naming the blocked use.

10.2.2.9 Lesson 9: Historical extraction-and-termination ethics

Concept. Historical extraction-and-termination ethics uses the historical motif to discuss source-protection ethics, documentation, and oversight without recreating handling procedures.

Why it matters. Without explicit treatment of **Historical extraction-and-termination ethics**, opportunistic collection undermines requirements decomposition and source-discipline fit review; the lesson builds the habit to separate collection discipline concepts from operational recruitment, interception, or tasking procedures.

Source support. Historical extraction-and-termination ethics rests on [029, 2026] and [004, 2026]. The most specific cited work observes: It surveys the roles of case officers in managing sources, recruitment and training of agents, protective measures such as fronts and cutouts, agent classifications including unwitting sources, and counterintelligence methods for identifying foreign operatives and reducing security breaches. Use them for the claim that **Historical extraction-and-termination ethics** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. For **Historical extraction-and-termination ethics**, work from the cited evidence behind this row. [029, 2026] A roughly 28-page Scribd document titled "Agent Handling in Counterintelligence" providing an educational overview of intelligence operations. It surveys the roles of case officers in managing sources, recruitment and training of agents, protective measures such as fronts and cutouts, agent classifications including unwitting sources, and counterintelligence methods for identifying foreign operatives and reducing security breaches. [004, 2026] Tom Mulligan argues that artificial intelligence will enhance rather than replace human intelligence professionals, contending that the future of intelligence lies in human-machine collaboration. He maintains that uniquely human qualities such as intuition, experience, and independent judgment become more valuable as adversaries gain access to the same AI tools. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. Build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must cite the historical descriptor, the bounded lesson about **Historical extraction-and-termination ethics**, the handling caveat, the uncertainty note, the protected-tradecraft boundary, and the reviewer who clears the account. Shape this subject work as a **source-risk and validation ethics worksheet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Historical extraction-and-termination ethics**: that a documented handling precedent licenses repeating the approach, rather than a case-bound record whose risks must be re-assessed each time.

Transfer task. Apply this module's safe boundary for **Historical extraction-and-termination ethics** to another artifact while keeping requirements decomposition and source-discipline fit and reviewer ownership explicit.

10.2.2.10 Lesson 10: Declassified source-protection and agent-handling ethics

Concept. Declassified source-protection and agent-handling ethics studies the declassified record for institutional lessons about oversight, source protection, and limits on translating history into practice.

Why it matters. Declassified source-protection connects classroom vocabulary to Collection Management and Multi-INT Requirements Discipline practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Declassified source-protection and agent-handling ethics rests on [032, 2026]. The most specific cited work observes: The 144-page volume is presented as a historical document on Soviet human-intelligence doctrine and counterintelligence practice. Use it for fixing what **Declassified source-protection and agent-handling ethics** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. Read **Declassified source-protection** against the works cited for this row. [032, 2026] A Google Books catalog entry for a 2025 English-translation edition of a Cold War-era Soviet intelligence training manual, published by Century Print Media Group with a translator's note by a retired NATO intelligence officer. The 144-page volume is presented as a historical document on Soviet human-intelligence doctrine and counterintelligence practice. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. Build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must cite the declassified source descriptor, the bounded lesson about **Declassified source-protection**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape this subject work as a **source-risk and validation ethics worksheet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Declassified source-protection**: that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Reuse the **Declassified source-protection** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

10.2.2.11 Lesson 11: AI-Enhanced Micro-Expression Analysis for Source Validation

Concept. AI-Enhanced Micro-Expression Analysis for Source Validation connects source-protection duties to reporting quality, compartmentation, and counterintelligence review without recreating handling tradecraft.

Why it matters. AI-Enhanced Micro-Expression Analysis connects classroom vocabulary to Collection Management and Multi-INT Requirements Discipline practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. AI-Enhanced Micro-Expression Analysis for Source Validation rests on [004, 2026]. Its anchor reference records: Tom Mulligan argues that artificial intelligence will enhance rather than replace human intelligence professionals, contending that the future of intelligence lies in human-machine collaboration. Use it for fixing what **AI-Enhanced Micro-Expression Analysis for Source Validation** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. Read **AI-Enhanced Micro-Expression Analysis** against the works cited for this row. [004, 2026] Tom Mulligan argues that artificial intelligence will enhance rather than replace human intelligence professionals, contending that the future of intelligence lies in human-machine collaboration. He maintains that uniquely human qualities such as intuition, experience, and independent judgment become more valuable as adversaries gain access to the same AI tools. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **AI-Enhanced Micro-Expression Analysis**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must name the source descriptor, the bounded claim about **AI-Enhanced Micro-Expression Analysis for Source**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **AI-Enhanced Micro-Expression Analysis** work as a **source-risk and validation ethics worksheet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that AI-Enhanced Micro-Expression Analysis for Source Validation replaces human review whenever evidence looks plausible.

Transfer task. Transfer **AI-Enhanced Micro-Expression Analysis** to a second module by preserving requirements decomposition and source-discipline fit, changing the source evidence, and naming a new reviewer.

10.2.2.12 Lesson 12: Digital-age recruitment-risk and consent-boundary

Concept. Digital-age recruitment-risk and consent-boundary reads recruitment doctrine as risk literacy: pressure, consent, validation, and the line that blocks operational contact.

Why it matters. Without explicit treatment of **Digital-age recruitment-risk**, confusing motivation literacy with contact authorization undermines requirements decomposition and source-discipline fit review; the lesson builds the habit to separate collection discipline concepts from operational recruitment, interception, or tasking procedures.

Source support. Digital-age recruitment-risk and consent-boundary rests on [004, 2026]. The lead source's own note reads: He maintains that uniquely human qualities such as intuition, experience, and independent judgment become more valuable as adversaries gain access to the same AI tools. Use it for pinning down the scope of **Digital-age recruitment-risk and consent-boundary**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. Read **Digital-age recruitment-risk** against the works cited for this row. [004, 2026] Tom Mulligan argues that artificial intelligence will enhance rather than replace human intelligence professionals, contending that the future of intelligence lies in human-machine collaboration. He maintains that uniquely human qualities such as intuition, experience, and independent judgment become more valuable as adversaries gain access to the same AI tools. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. Build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must note the motivation descriptor, the bounded claim about **Digital-age recruitment-risk**, the consent caveat, the uncertainty note, the no-contact boundary, and the reviewer who owns escalation duties. Shape this subject work as a **source-risk and validation ethics worksheet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Digital-age recruitment-risk**: that motivation literacy is contact authorization.

Transfer task. Transfer **Digital-age recruitment-risk** from this module to a second motif by preserving requirements decomposition and source-

discipline fit, replacing action with audit, and naming the blocked use.

10.2.3 Agent Handling and Management worked safe example: synthetic inputs, evidence, and review

Worked example: a synthetic policy cell compares public indicators of hybrid pressure against an approved collection plan for a benign border-disruption exercise. [239, 2026]; [240, 2026].

Triangulation anchors. In module 5's worked-example section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **human-source literacy and source protection**. Learners use a **source-risk and validation ethics worksheet** and keep this boundary visible: No elicitation, impersonation, covert contact, or operational source-management procedures; all cases use classroom fixtures.

Frame. The classroom question centers on **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust**. Excluded actions stay explicit, and the **Requirements-to-Evidence Lens** planning question is: What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit?

Inputs. For the **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust** scenario, use public notices, synthetic interview summaries, public logistics records, and an instructor scope card. The Requirements-to-Evidence Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust**, students rank requirements, choose the least intrusive source discipline, list excluded actions, and evaluate evidence quality. Pause whenever an inference about The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust** classroom scenario; unit artifact = source-risk and validation ethics worksheet; evidence = allowed inputs; method = requirements decomposition and source-discipline fit; output = a requirements-to-evidence matrix with discipline fit, source caveats, minimization notes, and gaps; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust** as "Requirements-to-Evidence Lens confirms it" is not enough. The revision ties the claim to requirements decomposition and source-discipline fit, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

10.2.4 Agent Handling and Management practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Requirements-to-Evidence Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**.

Triangulation anchors. In module 5's practice-sequence section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust, Historical meeting-structure ethics, Historical surveillance-risk and source-protection; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Collection Management and Multi-INT Requirements Discipline** lane.
2. Frame	Answer the lens question: What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust: requirements matrix with source descriptors, caveats, and collection limits.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the source-risk and validation ethics worksheet fields for The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust.	Unit profile note.	Evidence artifacts include validation note, pressure-risk checklist.
4. Challenge	Test the misconception that The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust is optional whenever separate collection discipline concepts from operational recruitment, interception, or tasking procedures feels inconvenient.	Failure-mode note.	The artifact applies the key distinction: separate collection discipline concepts from operational recruitment, interception, or tasking procedures.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

10.2.4.1 Agent Handling and Management instructor notes: source reasoning, review points, and studio focus Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor

or a human review point. Keep the focus on **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**. [239, 2026]; [240, 2026].

10.2.4.2 Agent Handling and Management extension exercise: peer validation and refresh trigger review **Evidence anchor.** Section 10; [239, 2026].
Have learners swap artifacts and apply the **Requirements-to-Evidence Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**.

10.2.5 Agent Handling and Management knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 10; [239, 2026].

1. Explain how **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust** is defined here; name the source descriptor that supports the definition.
2. Contrast **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust** with **Historical meeting-structure ethics** using the **Requirements-to-Evidence Lens** artifact fields.
3. Identify one failure mode from the **Collection Management and Multi-INT Requirements Discipline** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which gray-zone indicator changes the least-intrusive source choice without crossing into operational tasking?
5. Correct this misconception: that The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust is optional whenever separate collection discipline concepts from operational recruitment, interception, or tasking procedures feels inconvenient.

10.2.5.1 Agent Handling and Management answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust** without source evidence, uncertainty, or a safe transfer task.

10.3 Agent Handling and Management assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 10; [239, 2026].

10.3.1 Agent Handling and Management evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 10; [239, 2026].

10.3.2 Agent Handling and Management transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 10; [239, 2026].

10.3.2.1 Agent Handling and Management lineage and source tradition: profile, concepts, and first anchors This sits in the **Collection Management and Multi-INT Requirements Discipline** lineage: requirements-driven, authority-bounded collection where priorities, legal basis, minimization, source protection, and evaluation are explicit. [239, 2026]; [240, 2026].

10.3.2.2 Agent Handling and Management working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 10; [239, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**, with provenance and reviewability throughout.

10.3.2.3 Agent Handling and Management knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** accountable requirements, source-discipline choices, minimization rules, source-risk notes, and evaluation criteria. [239, 2026]; [240, 2026].
- **Transforms:** priority mapping, source-discipline fit, least-intrusive evidence selection, and feedback review.
- **Outputs:** requirements matrix, collection-limit note, source-quality card, and gap list.
- **Failure modes:** recruitment or interception drift, over-collection, weak minimization, and source exposure.

10.3.2.4 Agent Handling and Management transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 10; [239, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**.
- **Evidence contract:** keep the **Collection Management and Multi-INT Requirements Discipline** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as requirements matrix, collection-limit note, source-quality card, and gap list that another reviewer can audit.

10.3.2.5 Agent Handling and Management profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 10; [239, 2026].

The matched profile emphasizes requirements-driven, authority-bounded collection where priorities, legal basis, minimization, source protection, and evaluation are explicit. The method stack is priority mapping, requirement decomposition, source-discipline fit, coverage-gap review, legal-authority check, and collection-feedback loop; the local topic cluster is **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**.

10.3.3 Agent Handling and Management evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 10; [239, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Collection Management and Multi-INT Requirements Discipline** profile tells reviewers what evidence is strong enough for the module artifact built around **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**.

10.3.3.1 Agent Handling and Management guide source spine: inherited keys and local citation roles Primary guide citations: [239, 2026]; [240, 2026]; [241, 2026]; [273, 2026]; [276, 2026]; [285, 2026]; [286, 2026]; [290, 2026]; [294, 2026]; [025, 2026]; [029, 2026]; [004, 2026]; [026, 2026]; [016, 2026]; [027, 2026]; [028, 2026]; [030, 2026]; [031, 2026]; [032, 2026].

10.3.3.2 Agent Handling and Management verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [239, 2026]; [240, 2026].

Tier	What counts	How it is used
Source guide	[239, 2026]; [240, 2026]; [241, 2026]; [273, 2026]; [276, 2026]; [285, 2026]; [286, 2026]; [290, 2026]; [294, 2026]; [025, 2026]; [029, 2026]; [004, 2026]; [026, 2026]; [016, 2026]; [027, 2026]; [028, 2026]; [030, 2026]; [031, 2026]; [032, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 5's source-canon section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics** and [239, 2026]; [240, 2026], but only directly verified source URLs are encoded as citations.

10.3.3.3 Agent Handling and Management intelligence practice lens: evidence artifact and safety check Practice lens: **Requirements-to-Evidence Lens** for **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**. [239, 2026]; [240, 2026].

Planning question: What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit?

Evidence artifact: requirements matrix with source descriptors, caveats, and collection limits.

Validation rule: show priority, authority, minimization, corroboration, and source quality before any claim is reused. Applied to **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**.

Handoff contract: deliver metadata-rich evidence packets, not unscoped data piles or implicit targeting requests.

Safety check: exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure.

10.3.3.4 Agent Handling and Management runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 10; [239, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	5.99	5.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Agent Handling and Management to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Bounded autonomy, procurement, incident-response, and assurance studio	5.101	5.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Agent Handling and Management	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Model-card, recoverability, retention, and learner-support evidence package	5.102	5.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Agent Handling and Management	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust	5.1	5.1 The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Historical meeting-structure ethics	5.2	5.2 source title transformed into safe curriculum treatment; original: Meeting Structures: Overt, Covert, and Clandestine	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Historical surveillance-risk and source-protection	5.3	5.3 source title transformed into safe curriculum treatment; original: The Surveillance Detection Route (SDR)	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Historical clandestine-communications ethics	5.4	5.4 source title transformed into safe curriculum treatment; original: Dead Drops: Physical and Digital Methods	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Historical cutout-and-intermediary provenance	5.5	5.5 source title transformed into safe curriculum treatment; original: Cutouts, Intermediaries, and Deniability Chains	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Historical front-entity provenance	5.6	5.6 source title transformed into safe curriculum treatment; original: Fronts and Shell Entities as Agent Infrastructure	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Historical surveillance-risk and source-protection	5.7	5.7 source title transformed into safe curriculum treatment; original: Counter-Surveillance and Detecting Hostile Surveillance	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Historical agent-tasking oversight	5.8	5.8 source title transformed into safe curriculum treatment; original: Running Agents-in-Place: Frequency, Tasking, Validation	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Historical extraction-and-termination ethics	5.9	5.9 source title transformed into safe curriculum treatment; original: Burning, Exfiltrating, and Terminating Agents	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Declassified source-protection and agent-handling ethics	5.10	5.10 source title transformed into safe curriculum treatment; original: KGB Working-with-Agents Doctrine (Declassified Manuals)	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
AI-Enhanced Micro-Expression Analysis for Source Validation	5.11	5.11 AI-Enhanced Micro-Expression Analysis for Source Validation	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Digital-age recruitment-risk and consent-boundary	5.12	5.12 source title transformed into safe curriculum treatment; original: AI-Personalized Communication: Tailoring Persuasion to Source Personality	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

10.3.3.5 Agent Handling and Management reusable subsection contract: topic rows, artifacts, and safety duties **Evidence anchor.** Section 10; [239, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Historical meeting-structure ethics	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Historical surveillance-risk and source-protection	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Historical clandestine-communications ethics	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Historical cutout-and-intermediary provenance	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Historical front-entity provenance	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Counter-Surveillance and Detecting Hostile Surveillance: Historical surveillance-risk and source-protection	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Historical agent-tasking oversight	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Historical extraction-and-termination ethics	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Declassified source-protection and agent-handling ethics	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
AI-Enhanced Micro-Expression Analysis for Source Validation	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Digital-age recruitment-risk and consent-boundary	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

10.3.3.6 Agent Handling and Management annotated source ledger: real titles and local contribution Each source cited by this **Collection Management and Multi-INT Requirements Discipline** module is paired below with its real title and a one-line note on what it contributes to **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**.

Source	Cited work	What it contributes	Status
[239, 2026]	Digital Space and Human Rights	Official OHCHR digital rights portal.	original source-guide
[240, 2026]	The Right to Privacy in the Digital Age	The Office of the High Commissioner for Human Rights (OHCHR) hub page on the right to privacy in the digital age. It addresses how data-intensive technologies, particularly artificial intelligence, create risks for privacy, autonomy, and human dignity, and curates international standards, reports, and expert consultations.	verified source-guide
[241, 2026]	Modernised Convention 108	Official Council of Europe Convention 108+ source.	original source-guide

Source	Cited work	What it contributes	Status
[273, 2026]	WCAG 2 Overview	The W3C Web Accessibility Initiative overview of the Web Content Accessibility Guidelines (WCAG), an international standard for making web content accessible to people with disabilities. It explains that WCAG is organized around four principles (perceivable, operable, understandable, robust) with testable success criteria at three conformance levels (A, AA, AAA), and covers versions 2.0, 2.1, and 2.2.	verified source-guide
[276, 2026]	What is a Data Protection Impact Assessment and When Is This Mandatory?	A European Data Protection Board FAQ page, part of its data protection guide for small businesses, explaining Data Protection Impact Assessments (DPIAs) and when they are mandatory. It describes a DPIA as a written assessment of the impact of a planned processing operation, required when processing poses high risks to individuals' rights.	verified source-guide
[285, 2026]	NIST AI Resource Center	The NIST AI Resource Center (AIRC), a government platform supporting implementation of the NIST AI Risk Management Framework, a voluntary framework for managing AI risk. It provides the core framework along with a playbook of practical actions, profiles tailored to specific sectors and technologies, use cases, and crosswalks linking the framework to other governance structures.	verified source-guide
[286, 2026]	Model Cards for Model Reporting	The arXiv abstract for "Model Cards for Model Reporting" (2018) by Mitchell, Wu, Zaldivar, and colleagues, which introduces a framework for transparent documentation of machine learning models. Model cards are short accompanying documents that report a model's benchmarked performance across varied conditions, including different cultural, demographic, and phenotypic groups, along with intended use, evaluation methodology, and deployment considerations.	verified source-guide
[290, 2026]	NIST SP 800-218A: Secure Software Development Practices for Generative AI and Dual-Use Foundation Models	NIST Special Publication 800-218A (July 2024), which augments the Secure Software Development Framework with practices specific to AI model development across the software lifecycle. Produced in response to Executive Order 14110, it addresses AI model producers, developers building on those models, and acquirers of AI systems, and is designed to be used alongside NIST SP 800-218.	verified source-guide
[294, 2026]	M-25-21: Accelerating Federal Use of AI through Innovation, Governance, and Public Trust	An April 2025 Office of Management and Budget memorandum (M-25-21) directing executive branch agencies on federal use of artificial intelligence. Issued under Executive Order 14179, it instructs agencies to accelerate adoption of AI to improve public services and government efficiency while maintaining safeguards for civil rights, civil liberties, and privacy.	verified source-guide

Source	Cited work	What it contributes	Status
[025, 2026]	Andrew Bustamante: Inside the Mind of a Spy — Tradecraft, Trust	This is an episode of The Unmistakable Creative Podcast featuring former CIA field operative Andrew Bustamante discussing intelligence work. The conversation covers his background at the Air Force Academy and CIA training, and frames espionage as resting on reading people, trust, influence, and empathy rather than glamour or action. It also addresses how operatives are selected, the isolation of covert work, and its psychological effects on personal relationships.	verified source-guide
[029, 2026]	Agent Handling in Counterintelligence / PDF	A roughly 28-page Scribd document titled "Agent Handling in Counterintelligence" providing an educational overview of intelligence operations. It surveys the roles of case officers in managing sources, recruitment and training of agents, protective measures such as fronts and cutouts, agent classifications including unwitting sources, and counterintelligence methods for identifying foreign operatives and reducing security breaches.	verified source-guide context; do not use as primary analytic support
[004, 2026]	AI Won't Replace Spies—It Will Make Them More Powerful Than Ever	Tom Mulligan argues that artificial intelligence will enhance rather than replace human intelligence professionals, contending that the future of intelligence lies in human-machine collaboration. He maintains that uniquely human qualities such as intuition, experience, and independent judgment become more valuable as adversaries gain access to the same AI tools.	verified source-guide
[026, 2026]	The tension and drama behind surveillance detection operations	A YouTube video titled "Inside the CIA: The tension and drama behind surveillance detection operations," released May 3, 2024, featuring a former CIA officer. The speaker describes the operational complexity and interpersonal tension involved in moving safely from a starting point to a meeting while accounting for the presence of hostile observation. It conveys the difficulty and stress of clandestine field meetings as recounted from personal experience.	verified source-guide
[016, 2026]	Surveillance Detection - State.gov	Place where victim can be controlled with limited avenues of escape.	original source-guide
[027, 2026]	The Dead Drop: Design a Communications Method Like a Spy	Learn a technique for communicating with your family in an emergency using a method used by spies.	original source-guide
[028, 2026]	Cited source (see bibliography)	See bibliography for scope.	original source-guide
[030, 2026]	The Secrets of Countersurveillance	See bibliography for scope.	original source-guide
[031, 2026]	KGB counter surveillance: How to know if you're being followed	There are cameras everywhere! Everything is trackable!	original source-guide
[032, 2026]	Cited source (see bibliography)	A Google Books catalog entry for a 2025 English-translation edition of a Cold War-era Soviet intelligence training manual, published by Century Print Media Group with a translator's note by a retired NATO intelligence officer. The 144-page volume is presented as a historical document on Soviet human-intelligence doctrine and counterintelligence practice.	verified source-guide

Where this sits. This module's overview is Section 10; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates

that govern this module.

10.3.4 Agent Handling and Management governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 10; [239, 2026].

10.3.5 Agent Handling and Management analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 5's governance-boundary section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **Collection Management and Multi-INT Requirements Discipline** for **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**. [239, 2026]; [240, 2026].

Curriculum topic spine: The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust, **Historical meeting-structure ethics**, **Historical surveillance-risk and source-protection**. **Verified anchor cluster:** [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]; [Archives and Administration, 1981]; [Agency, 2026g]; [of the Director of National Intelligence, 2026d].

Conceptual depth: requirements-driven, authority-bounded collection where priorities, legal basis, minimization, source protection, and evaluation are explicit.

Method stack: priority mapping, requirement decomposition, source-discipline fit, coverage-gap review, legal-authority check, and collection-feedback loop.

Composability contract: requirements, authorities, source disciplines, collection notes, retention limits, caveats, and evaluation metrics remain separable.

Known failure modes: opportunistic collection, priority drift, over-collection, weak minimization, source exposure, and confusing availability with authority.

Defensive boundary: collection material remains doctrinal and governance-oriented; it does not teach recruitment, interception, surveillance, or tasking procedures. Applied to **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**.

Anchor	Why it matters here
[Community, 2026]	Official public explanation of the intelligence cycle, collection disciplines, dissemination, evaluation, oversight, and partners. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026c]	Official prioritization directive for translating national intelligence priorities into collection, analysis, risk management, and responsiveness evaluation. Checked as of 2026-05-21; role: curriculum_anchor.
[of Staff, 2026]	Official joint-doctrine landing page for the keystone publication on joint intelligence principles, products, services, and assessments. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence and Agency, 2024]	Official IC OSINT strategy for professionalizing OSINT, integrated collection management, open-source sharing, innovation, and tradecraft. Checked as of 2026-05-21; role: curriculum_anchor.
[Archives and Administration, 1981]	Official legal anchor for intelligence authorities, rights-aware collection, analytic competition, oversight, and source-method protection. Checked as of 2026-05-21; role: curriculum_anchor.
[Agency, 2026g]	Official NSA public explanation of FISA oversight for signals intelligence collection governed by statutory and court-authorized controls. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026d]	Official sourcing directive for traceability, citations, source descriptors, and source summaries. Checked as of 2026-05-21; role: curriculum_anchor.

10.3.5.1 Agent Handling and Management evidence standard and citation floor: source families and discovery limits Official guidance supplies governance, safety, and legal constraints for the **Collection Management and Multi-INT Requirements Discipline** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [239, 2026]; [240, 2026].

10.3.6 Agent Handling and Management agentic boundary: assist, approve, block, and record

Evidence anchor. Section 10; [239, 2026].

AGEINT translation is bounded by the **Collection Management and Multi-INT Requirements Discipline** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**.

10.3.6.1 Agent Handling and Management permitted defensive utility: curriculum uses and safe outputs **Evidence anchor.** Section 10; [239, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**.

10.3.6.2 Agent Handling and Management excluded operational boundary: blocked actions and stop rules Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [239, 2026]; [240, 2026] and **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

10.3.7 Agent Handling and Management governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 10; [239, 2026].

Governance is practiced as a gate on the **Collection Management and Multi-INT Requirements Discipline** lane. Learners use the **Requirements-to-Evidence Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**.

10.3.7.1 Agent Handling and Management governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [239, 2026]; [240, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Collection Management and Multi-INT Requirements Discipline** failure modes and the **Requirements-to-Evidence Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

10.3.7.2 Agent Handling and Management evidence package handoff: appendices, records, and reuse

Evidence anchor. Section 10; [239, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Requirements-to-Evidence Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**.

10.3.7.3 Agent Handling and Management current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**. [239, 2026]; [240, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_intelligence_gov_how_ic_works` for **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**?	How the IC Works; lane `governed_intelligence_cycle`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official public explanation of the intelligence cycle, collection disciplines, dissemination, evaluation, oversight, and partners.
What does the module inherit from `official_odni_icd_204` for **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**?	Intelligence Community Directive 204: National Intelligence Priorities Framework; lane `collection_management`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official prioritization directive for translating national intelligence priorities into collection, analysis, risk management, and responsiveness evaluation.
What does the module inherit from `official_joint_pub_2_0` for **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**?	JP 2-0: Joint Intelligence; lane `collection_management`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official joint-doctrine landing page for the keystone publication on joint intelligence principles, products, services, and assessments.
What does the module inherit from `official_ic_osint_strategy` for **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**?	The INT of First Resort: The IC OSINT Strategy 2024-2026; lane `osint_geoint`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official IC OSINT strategy for professionalizing OSINT, integrated collection management, open-source sharing, innovation, and tradecraft.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 10; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

10.3.8 Agent Handling and Management assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 10; [239, 2026].

10.3.9 Agent Handling and Management assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 10; [239, 2026].

10.3.9.1 Agent Handling and Management capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics** and [239, 2026]; [240, 2026].

10.3.9.2 Agent Handling and Management instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics** and [239, 2026]; [240, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

10.3.9.3 Agent Handling and Management assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust	Completed **requirements matrix with source descriptors, caveats, and collection limits** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Historical meeting-structure ethics	Completed **requirements matrix with source descriptors, caveats, and collection limits** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Historical surveillance-risk and source-protection	Completed **requirements matrix with source descriptors, caveats, and collection limits** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

10.3.10 Agent Handling and Management refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [239, 2026]; [240, 2026] and **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**.

10.3.10.1 Agent Handling and Management refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**. The local signals begin with [239, 2026]; [240, 2026].

10.3.10.2 Agent Handling and Management claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**, and the source spine for these checks begins with [239, 2026]; [240, 2026].

10.3.11 Agent Handling and Management reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [239, 2026]; [240, 2026].

Triangulation anchors. In module 5's review-checklist section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics**. [239, 2026]; [240, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

10.3.12 Agent Handling and Management learning-path links: module map, overview, and curriculum atlas

Follow the cross-links to move between **The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust; Historical meeting-structure ethics** and the rest of the curriculum without losing the source spine: orientation first, then the parent unit, then the modules on either side. Primary sources: [239, 2026]; [240, 2026].

Section 2, Section 8, Section 9, Section 11

11 Source Protection and CI Integration

11.0.1 Source Protection and CI Integration figures and course links: visual evidence, source flow, and navigation

The module uses Figure 40 and Figure 36 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 8, Section 10, Section 12.
This module teaches the **Collection Management and Multi-INT Requirements Discipline** lane through a bounded, source-backed coursebook chapter. [238, 2026]; [241, 2026].

11.1 Collection Management and Multi-INT Requirements Discipline frame for Source Protection and CI Integration: source context, topic focus, and reader task

Evidence anchor. Section 11; [238, 2026].

11.1.1 Source Protection and CI Integration orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 11; [238, 2026].

11.1.2 Source Protection and CI Integration conceptual primer: source context, core model, and reader task

This chapter teaches collection management as requirements discipline: a source method is considered only after the priority, authority, minimization rule, source risk, and evaluation plan are explicit. The chapter uses **Requirements-to-Evidence Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**.
The central distinction is to separate collection discipline concepts from operational recruitment, interception, or tasking procedures. Core topics include **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance; Lie Detection, Vetting, Polygraph, and Its Alternatives**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [238, 2026]; [241, 2026].
Learners move from vocabulary and the **Requirements-to-Evidence Lens** distinction through topic lessons on **Identifying Penetration: Signs of Compromise** with evidence and misconception checks, then assemble a **requirements matrix with source descriptors, caveats, and collection limits** with safety and rights gates.

11.1.3 Source Protection and CI Integration learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 11; [238, 2026].

- Connect **Identifying Penetration: Signs of Compromise and Compartmentation and need-to-know governance** to **Collection Management and Multi-INT Requirements Discipline** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **requirements matrix with source descriptors, caveats, and collection limits** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate collection discipline concepts from operational recruitment, interception, or tasking procedures; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as opportunistic collection, priority drift, over-collection, weak minimization, source exposure, and confusing availability with authority, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: collection material remains doctrinal and governance-oriented; it does not teach recruitment, interception, surveillance, or tasking procedures.

11.1.4 Source Protection and CI Integration core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 11; [238, 2026].

Term	Working definition
Priority	the relative importance of an intelligence question
Source discipline	a broad evidence channel such as HUMINT, SIGINT, GEOINT, OSINT, or FININT
Minimization	the rule that limits acquisition, retention, or use of unnecessary information
Source protection	the duty to reduce risk to people, methods, and sensitive relationships
Evaluation	the feedback step that tests whether the evidence satisfied the requirement
Gray-zone indicator	an observable signal of ambiguous coercion below armed conflict thresholds
Proxy pattern	a relationship suggesting indirect sponsorship without confirmed operational control
Identifying Penetration: Signs of Compromise	Key terms: Identifying, Penetration, Signs.
Compartmentation and need-to-know governance	Key terms: Compartmentation, need, know.

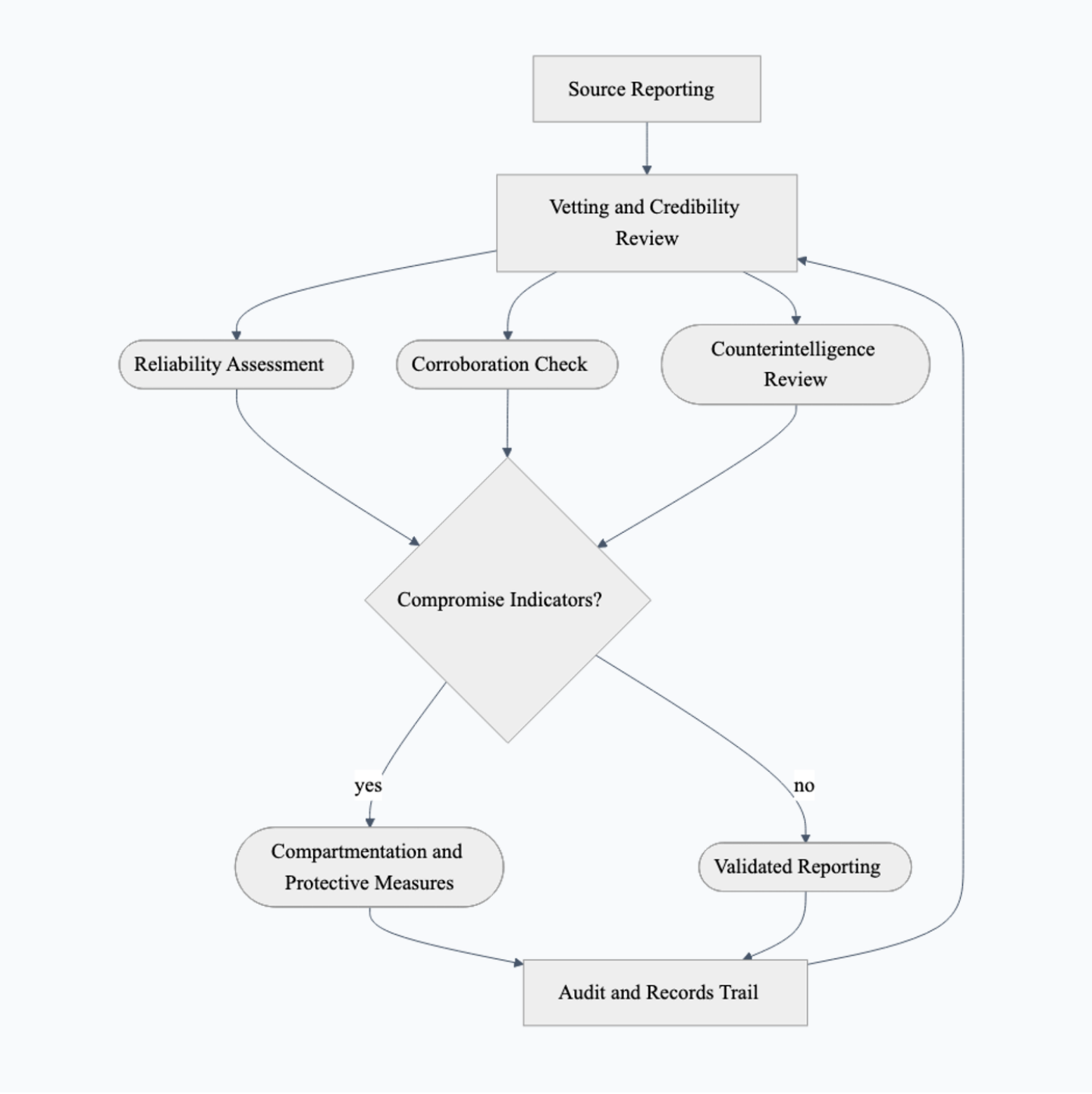


Figure 40: This diagram teaches the defensive governance flow that evaluates source reliability and protects sources through compartmentation and counterintelligence review. Its reader value is to make Source Reporting, Vetting and Credibility Review, and Audit and Records Trail visible at a glance, with the human intelligence humint / source protection and ci integration section as the source section and defensive review as the boundary.

11.2 Requirements-to-Evidence Lens path for Source Protection and CI Integration: lesson cluster, safe artifact, and review

Evidence anchor. Section 11; [238, 2026].

11.2.1 Source Protection and CI Integration practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 11; [238, 2026].

11.2.2 Source Protection and CI Integration topic lessons: source-backed concepts and transfer tasks

This module builds collection management as requirements discipline: a source method is considered only after the priority, authority, minimization rule, source risk, and evaluation plan are explicit. The sequence opens with **Identifying Penetration: Signs of Compromise**, **Compartmentation and need-to-know governance**, **Lie Detection, Vetting, Polygraph, and Its Alternatives** and applies the **Requirements-to-Evidence Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 36; module overview Section 11; curriculum atlas Section 2.

Triangulation anchors. In module 6's topic-lessons section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

11.2.2.1 Lesson 1: Identifying Penetration: Signs of Compromise

Concept. Identifying Penetration: Signs of Compromise applies Identifying, Penetration, Signs within Collection Management and Multi-INT Requirements Discipline: learners use separate collection discipline concepts from operational recruitment, interception, or tasking procedures and requirements decomposition and source-discipline fit evidence before any judgment moves forward.

Why it matters. Identifying Penetration connects classroom vocabulary to Collection Management and Multi-INT Requirements Discipline practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Identifying Penetration: Signs of Compromise rests on [307, 2026], [305, 2026], and [304, 2026]. Its anchor reference records: NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Use them for fixing what **Identifying Penetration: Signs of Compromise** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. Read **Identifying Penetration** against the works cited for this row. [307, 2026] Official CISA Industrial Control Systems recommended practices page for defensive ICS/OT safety, resilience, and incident-preparation guidance. [305, 2026] Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Identifying Penetration**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must name the source descriptor, the bounded claim about **Identifying Penetration**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Identifying Penetration** work as a **source-risk and validation ethics worksheet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that Identifying Penetration: Signs of Compromise can be used while ignoring the rule to separate collection discipline concepts from operational recruitment, interception, or tasking procedures.

Transfer task. Transfer **Identifying Penetration** to a second module by preserving requirements decomposition and source-discipline fit, changing the source evidence, and naming a new reviewer.

11.2.2.2 Lesson 2: Compartmentation and need-to-know governance

Concept. Compartmentation and need-to-know governance treats agents as software actors with explicit permissions, logs, stop conditions, and human approval—not autonomous decision makers.

Why it matters. Compartmentation and need-to-know governance connects classroom vocabulary to Collection Management and Multi-INT Requirements Discipline practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Compartmentation and need-to-know governance rests on [029, 2026]. The closest source to this row notes: It surveys the roles of case officers in managing sources, recruitment and training of agents, protective measures such as fronts and cutouts, agent classifications including unwitting sources, and counterintelligence methods for identifying foreign operatives and reducing security breaches. Use it for pinning down the scope of **Compartmentation and need-to-know governance**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. Ground **Compartmentation and need-to-know governance** in the evidence the row cites. [029, 2026] A roughly 28-page Scribd document titled "Agent Handling in Counterintelligence" providing an educational overview of intelligence operations. It surveys the roles of case officers in managing sources, recruitment and training of agents, protective measures such as fronts and cutouts, agent classifications including unwitting sources, and counterintelligence methods for identifying foreign operatives and reducing security breaches. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. Build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must name the governance descriptor, the bounded claim about **Compartmentation and need-to-know governance**, the compartmentation caveat, the uncertainty note, the non-authorization boundary, and the reviewer who signs oversight. Shape this subject work as a **source-risk and validation ethics worksheet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Compartmentation and need-to-know governance**: that governance vocabulary about tradecraft confers operational authorization rather than the constraints under which any action must be approved.

Transfer task. Reuse the **Compartmentation and need-to-know governance** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

11.2.2.3 Lesson 3: Lie Detection, Vetting, Polygraph, and Its Alternatives

Concept. Lie Detection, Vetting, Polygraph, and Its Alternatives connects insider-threat review to access control, behavior indicators, and accountable escalation paths.

Why it matters. Lie Detection, Vetting, Polygraph, and Its Alternatives connects classroom vocabulary to Collection Management and Multi-INT Requirements Discipline practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Lie Detection, Vetting, Polygraph, and Its Alternatives rests on [307, 2026], [305, 2026], and [304, 2026]. The closest source to this row notes: NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set

of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Use them for pinning down the scope of **Lie Detection, Vetting, Polygraph, and Its Alternatives**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. For **Lie Detection, Vetting, Polygraph, and Its Alternatives**, work from the cited evidence behind this row. [307, 2026] Official CISA Industrial Control Systems recommended practices page for defensive ICS/OT safety, resilience, and incident-preparation guidance. [305, 2026] Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Lie Detection, Vetting, Polygraph, and Its Alternatives**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must name the source descriptor, the bounded claim about **Lie Detection Vetting Polygraph and**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape this subject work as a **source-risk and validation ethics worksheet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that Lie Detection, Vetting, Polygraph, and Its Alternatives establishes intent without reviewing alternative explanations.

Transfer task. Transfer **Lie Detection, Vetting, Polygraph, and Its Alternatives** to a second module by preserving requirements decomposition and source-discipline fit, changing the source evidence, and naming a new reviewer.

11.2.2.4 Lesson 4: The Double-Agent Operation

Concept. The Double-Agent Operation treats agents as software actors with explicit permissions, logs, stop conditions, and human approval—not autonomous decision makers.

Why it matters. Without explicit treatment of **The Double-Agent Operation**, opportunistic collection undermines requirements decomposition and source-discipline fit review; the lesson builds the habit to separate collection discipline concepts from operational recruitment, interception, or tasking procedures.

Source support. The Double-Agent Operation rests on [029, 2026]. The most specific cited work observes: A roughly 28-page Scribd document titled "Agent Handling in Counterintelligence" providing an educational overview of intelligence operations. Use it for the working definition that **The Double-Agent Operation** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. Read **The Double-Agent Operation** against the works cited for this row. [029, 2026] A roughly 28-page Scribd document titled "Agent Handling in Counterintelligence" providing an educational overview of intelligence operations. It surveys the roles of case officers in managing sources, recruitment and training of agents, protective measures such as fronts and cutouts, agent classifications including unwitting sources, and counterintelligence methods for identifying foreign operatives and reducing security breaches. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **The Double-Agent Operation**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must name the source descriptor, the bounded claim about **Double-Agent Operation**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape this subject work as a **source-risk and validation ethics worksheet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that The Double-Agent Operation replaces human review whenever evidence looks plausible.

Transfer task. Transfer **The Double-Agent Operation** to a second module by preserving requirements decomposition and source-discipline fit, changing the source evidence, and naming a new reviewer.

11.2.2.5 Lesson 5: Non-state actor indicator review with attribution caution and governance boundaries

Concept. Non-state actor indicator review with attribution caution and governance boundaries uses attribution indicators cautiously by separating technical similarity, context, confidence, and geopolitical inference.

Why it matters. Without explicit treatment of **Non-state actor indicator review**, opportunistic collection undermines requirements decomposition and source-discipline fit review; the lesson builds the habit to separate collection discipline concepts from operational recruitment, interception, or tasking procedures.

Source support. Non-state actor indicator review with attribution caution and governance boundaries rests on [033, 2026]. The lead source's own note reads: How seriously is the U.S. Use it for the claim that **Non-state actor indicator review with attribution caution and governance boundaries** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. For **Non-state actor indicator review**, work from the cited evidence behind this row. [033, 2026] How seriously is the U.S. Intelligence Community (IC) considering this challenge to U.S. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Non-state actor indicator review**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must name the actor descriptor, the bounded claim about **state actor indicator review with**, the attribution caveat, the uncertainty note, the non-targeting boundary, and the reviewer who approves the assessment. Shape **Non-state actor indicator review** work as a **source-risk and validation ethics worksheet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that lacking a state sponsor places an actor outside the reach of governance, accountability, and applicable rules.

Transfer task. Reuse the **Non-state actor indicator review** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

11.2.2.6 Lesson 6: Espionage in the AI Era: Why HUMINT Will Grow in Importance

Concept. Espionage in the AI Era: Why HUMINT Will Grow in Importance treats human-source work as a governed relationship: validation, consent, reporting, source protection, and oversight—not contact activity.

Why it matters. Without explicit treatment of **Espionage in the AI Era: Why HUMINT Will Grow in Importance**, opportunistic collection undermines requirements decomposition and source-discipline fit review; the lesson builds the habit to separate collection discipline concepts from operational recruitment, interception, or tasking procedures.

Source support. Espionage in the AI Era: Why HUMINT Will Grow in Importance rests on [019, 2026] and [034, 2026]. The closest source to this row notes: By Thomas Mulligan, a researcher at the RAND Corporation who served in CIA during 2008–14. Use them for pinning down the scope of **Espionage in the AI Era: Why HUMINT Will Grow in Importance**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. Ground **Espionage in the AI Era: Why HUMINT Will Grow in Importance** in the evidence the row cites. [019, 2026] By Thomas Mulligan, a researcher at the RAND Corporation who served in CIA during 2008–14. [034, 2026] Thomas Mulligan is a researcher at the RAND Corporation and former CIA officer. Ana P. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Espionage in the AI Era**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must name the source descriptor, the bounded claim about **Espionage in the AI Era**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Espionage in the AI Era: Why HUMINT Will Grow in Importance** work as a **source-risk and validation ethics worksheet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that Espionage in the AI Era: Why HUMINT Will Grow in Importance is optional whenever separate collection discipline concepts from operational recruitment, interception, or tasking procedures feels inconvenient.

Transfer task. Transfer **Espionage in the AI Era: Why HUMINT Will Grow in Importance** to a second module by preserving requirements decomposition and source-discipline fit, changing the source evidence, and naming a new reviewer.

11.2.3 Source Protection and CI Integration worked safe example: synthetic inputs, evidence, and review

Worked example: a synthetic policy cell compares public indicators of hybrid pressure against an approved collection plan for a benign border-disruption exercise. [238, 2026]; [241, 2026].

Triangulation anchors. In module 6's worked-example section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **human-source literacy and source protection**. Learners use a **source-risk and validation ethics worksheet** and keep this boundary visible: No elicitation, impersonation, covert contact, or operational source-management procedures; all cases use classroom fixtures.

Frame. The classroom question centers on **Identifying Penetration: Signs of Compromise**. Excluded actions stay explicit, and the **Requirements-to-Evidence Lens** planning question is: What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit?

Inputs. For the **Identifying Penetration: Signs of Compromise** scenario, use public notices, synthetic interview summaries, public logistics records, and an instructor scope card. The Requirements-to-Evidence Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Identifying Penetration: Signs of Compromise**, students rank requirements, choose the least intrusive source discipline, list excluded actions, and evaluate evidence quality. Pause whenever an inference about Identifying Penetration: Signs of Compromise appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Identifying Penetration: Signs of Compromise** classroom scenario; unit artifact = source-risk and validation ethics worksheet; evidence = allowed inputs; method = requirements decomposition and source-discipline fit; output = a requirements-to-evidence matrix with discipline fit, source caveats, minimization notes, and gaps; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Identifying Penetration: Signs of Compromise** as "Requirements-to-Evidence Lens confirms it" is not enough. The revision ties the claim to requirements decomposition and source-discipline fit, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Identifying Penetration: Signs of Compromise** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

11.2.4 Source Protection and CI Integration practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Requirements-to-Evidence Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**.

Triangulation anchors. In module 6's practice-sequence section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Identifying Penetration: Signs of Compromise, Compartmentation and need-to-know governance, Lie Detection, Vetting, Polygraph, and Its Alternatives; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Collection Management and Multi-INT Requirements Discipline** lane.
2. Frame	Answer the lens question: What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Identifying Penetration: Signs of Compromise: requirements matrix with source descriptors, caveats, and collection limits.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the source-risk and validation ethics worksheet fields for Identifying Penetration: Signs of Compromise.	Unit profile note.	Evidence artifacts include validation note, pressure-risk checklist.

Move	Learner action	Output	Check
4. Challenge	Test the misconception that Identifying Penetration: Signs of Compromise can be used while ignoring the rule to separate collection discipline concepts from operational recruitment, interception, or tasking procedures.	Failure-mode note.	The artifact applies the key distinction: separate collection discipline concepts from operational recruitment, interception, or tasking procedures.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

11.2.4.1 Source Protection and CI Integration instructor notes: source reasoning, review points, and studio focus Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**. [238, 2026]; [241, 2026].

11.2.4.2 Source Protection and CI Integration extension exercise: peer validation and refresh trigger review Evidence anchor. Section 11; [238, 2026].

Have learners swap artifacts and apply the **Requirements-to-Evidence Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**.

11.2.5 Source Protection and CI Integration knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 11; [238, 2026].

1. Explain how **Identifying Penetration: Signs of Compromise** is defined here; name the source descriptor that supports the definition.
2. Contrast **Identifying Penetration: Signs of Compromise** with **Compartmentation and need-to-know governance** using the **Requirements-to-Evidence Lens** artifact fields.
3. Identify one failure mode from the **Collection Management and Multi-INT Requirements Discipline** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which gray-zone indicator changes the least-intrusive source choice without crossing into operational tasking?
5. Correct this misconception: that Identifying Penetration: Signs of Compromise can be used while ignoring the rule to separate collection discipline concepts from operational recruitment, interception, or tasking procedures.

11.2.5.1 Source Protection and CI Integration answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Identifying Penetration: Signs of Compromise** without source evidence, uncertainty, or a safe transfer task.

11.3 Source Protection and CI Integration assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 11; [238, 2026].

11.3.1 Source Protection and CI Integration evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 11; [238, 2026].

11.3.2 Source Protection and CI Integration transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 11; [238, 2026].

11.3.2.1 Source Protection and CI Integration lineage and source tradition: profile, concepts, and first anchors This sits in the **Collection Management and Multi-INT Requirements Discipline** lineage: requirements-driven, authority-bounded collection where priorities, legal basis, minimization, source protection, and evaluation are explicit. [238, 2026]; [241, 2026].

11.3.2.2 Source Protection and CI Integration working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 11; [238, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**, with provenance and reviewability throughout.

11.3.2.3 Source Protection and CI Integration knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** accountable requirements, source-discipline choices, minimization rules, source-risk notes, and evaluation criteria. [238, 2026]; [241, 2026].
- **Transforms:** priority mapping, source-discipline fit, least-intrusive evidence selection, and feedback review.
- **Outputs:** requirements matrix, collection-limit note, source-quality card, and gap list.
- **Failure modes:** recruitment or interception drift, over-collection, weak minimization, and source exposure.

11.3.2.4 Source Protection and CI Integration transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 11; [238, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**.
- **Evidence contract:** keep the **Collection Management and Multi-INT Requirements Discipline** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as requirements matrix, collection-limit note, source-quality card, and gap list that another reviewer can audit.

11.3.2.5 Source Protection and CI Integration profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 11; [238, 2026].

The matched profile emphasizes requirements-driven, authority-bounded collection where priorities, legal basis, minimization, source protection, and evaluation are explicit. The method stack is priority mapping, requirement decomposition, source-discipline fit, coverage-gap review, legal-authority check, and collection-feedback loop; the local topic cluster is **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**.

11.3.3 Source Protection and CI Integration evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 11; [238, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Collection Management and Multi-INT Requirements Discipline** profile tells reviewers what evidence is strong enough for the module artifact built around **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**.

11.3.3.1 Source Protection and CI Integration guide source spine: inherited keys and local citation roles Primary guide citations: [238, 2026]; [241, 2026]; [266, 2026]; [274, 2026]; [278, 2026]; [280, 2026]; [287, 2026]; [288, 2026]; [295, 2026]; [307, 2026]; [305, 2026]; [304, 2026]; [029, 2026]; [033, 2026]; [019, 2026]; [034, 2026].

11.3.3.2 Source Protection and CI Integration verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [238, 2026]; [241, 2026].

Tier	What counts	How it is used
Source guide	[238, 2026]; [241, 2026]; [266, 2026]; [274, 2026]; [278, 2026]; [280, 2026]; [287, 2026]; [288, 2026]; [295, 2026]; [307, 2026]; [305, 2026]; [304, 2026]; [029, 2026]; [033, 2026]; [019, 2026]; [034, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 6's source-canon section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance** and [238, 2026]; [241, 2026], but only directly verified source URLs are encoded as citations.

11.3.3.3 Source Protection and CI Integration intelligence practice lens: evidence artifact and safety check Practice lens: **Requirements-to-Evidence Lens** for **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**. [238, 2026]; [241, 2026].

Planning question: What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit?

Evidence artifact: requirements matrix with source descriptors, caveats, and collection limits.

Validation rule: show priority, authority, minimization, corroboration, and source quality before any claim is reused. Applied to **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**.

Handoff contract: deliver metadata-rich evidence packets, not unscoped data piles or implicit targeting requests.

Safety check: exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure.

11.3.3.4 Source Protection and CI Integration runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 11; [238, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	6.99	6.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Source Protection and CI Integration to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Bounded autonomy, procurement, incident-response, and assurance studio	6.101	6.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Source Protection and CI Integration	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Model-card, recoverability, retention, and learner-support evidence package	6.102	6.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Source Protection and CI Integration	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Identifying Penetration: Signs of Compromise	6.1	6.1 Identifying Penetration: Signs of Compromise	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Compartmentation and need-to-know governance	6.2	6.2 source title transformed into safe curriculum treatment; original: Compartmentation in Agent Networks	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Lie Detection, Vetting, Polygraph, and Its Alternatives	6.3	6.3 Lie Detection, Vetting, Polygraph, and Its Alternatives	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
The Double-Agent Operation	6.4	6.4 The Double-Agent Operation	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Non-state actor indicator review with attribution caution and governance boundaries	6.5	6.5 source title transformed into safe curriculum treatment; original: Hostile Intelligence from Non-State Actors	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Espionage in the AI Era: Why HUMINT Will Grow in Importance	6.6	6.6 Espionage in the AI Era: Why HUMINT Will Grow in Importance	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

11.3.3.5 Source Protection and CI Integration reusable subsection contract: topic rows, artifacts, and safety duties Evidence anchor. Section 11; [238, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Identifying Penetration: Signs of Compromise	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Compartmentation and need-to-know governance	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Lie Detection, Vetting, Polygraph, and Its Alternatives	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
The Double-Agent Operation	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Non-state actor indicator review with attribution caution and governance boundaries	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Espionage in the AI Era: Why HUMINT Will Grow in Importance	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

11.3.3.6 Source Protection and CI Integration annotated source ledger: real titles and local contribution Each source cited by this **Collection Management and Multi-INT Requirements Discipline** module is paired below with its real title and a one-line note on what it contributes to **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**.

Source	Cited work	What it contributes	Status
[238, 2026]	Recommendation on the Ethics of Artificial Intelligence	The official UNESCO page for the Recommendation on the Ethics of Artificial Intelligence, the first global standard-setting instrument on AI ethics, adopted in 2021 and applicable to all 194 member states. It outlines four core values, including human rights protection and environmental flourishing, and ten guiding principles such as proportionality, privacy, transparency, and fairness.	verified source-guide
[241, 2026]	Modernised Convention 108	Official Council of Europe Convention 108+ source.	original source-guide

Source	Cited work	What it contributes	Status
[266, 2026]	PROV Overview	A W3C Working Group Note from 2013 that provides an overview and roadmap for the PROV family of specifications for representing and exchanging provenance information on the web. It defines provenance as information about the entities, activities, and people involved in producing data, used to assess quality, reliability, and trustworthiness.	verified source-guide
[274, 2026]	CAST Universal Design for Learning Guidelines version 3.0	The official CAST website for the Universal Design for Learning (UDL) Guidelines version 3.0, released in 2024. The framework offers research-based guidance for designing inclusive learning environments and is organized around three principles: Engagement (motivation and emotional support), Representation (accessible presentation of information), and Action and Expression (diverse means of participation and communication).	verified source-guide
[278, 2026]	Recommendation of the Council on Public Procurement	The OECD Recommendation of the Council on Public Procurement (OECD/LEGAL/0411), a legal instrument adopted by the OECD Council in 2015 on the proposal of the Public Governance Committee. It frames public procurement as a pillar of strategic governance and service delivery and sets out principles for governments to follow.	verified source-guide
[280, 2026]	NIST SP 800-61 Rev. 3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management	NIST SP 800-61 Rev. 3, published April 2025, integrates incident response guidance into broader cybersecurity risk management aligned with the NIST Cybersecurity Framework 2.0, superseding the 2012 Rev. 2. The publication addresses cyber threat information sharing, incident handling and management practices, and procedures for detecting, responding to, and recovering from security incidents.	verified source-guide
[287, 2026]	Datasheets for Datasets	A 2018 arXiv paper proposing 'datasheets for datasets,' a standardized documentation framework for machine learning datasets modeled on electronic component datasheets. The authors argue the field lacks consistent dataset documentation, which creates risk in high-stakes applications, and propose that datasets be accompanied by documentation covering motivation, composition, collection process, recommended uses, and test results.	verified source-guide
[288, 2026]	Algorithmic Transparency Recording Standard Hub	A GOV.UK collection page serving as the hub for the UK Algorithmic Transparency Recording Standard (ATRS), maintained by the Government Digital Service. It provides a standardized template for documenting public-sector use of algorithmic tools, completion guidance, policy on scope and compliance, and a searchable repository of published transparency records.	verified source-guide

Source	Cited work	What it contributes	Status
[295, 2026]	M-25-22: Driving Efficient Acquisition of Artificial Intelligence in Government	OMB Memorandum M-25-22 (April 3, 2025), Driving Efficient Acquisition of Artificial Intelligence in Government, issued under Executive Order 13960 and related directives. It provides guidance to federal agencies for acquiring effective and trustworthy AI in a timely, cost-effective manner, and rescinds and replaces earlier memorandum M-24-18.	verified source-guide
[307, 2026]	ICS Recommended Practices	Official CISA Industrial Control Systems recommended practices page for defensive ICS/OT safety, resilience, and incident-preparation guidance.	original source-guide
[305, 2026]	DevSecOps	Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support.	original source-guide
[304, 2026]	Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities	NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences.	verified source-guide
[029, 2026]	Agent Handling in Counterintelligence / PDF	A roughly 28-page Scribd document titled “Agent Handling in Counterintelligence” providing an educational overview of intelligence operations. It surveys the roles of case officers in managing sources, recruitment and training of agents, protective measures such as fronts and cutouts, agent classifications including unwitting sources, and counterintelligence methods for identifying foreign operatives and reducing security breaches.	verified source-guide context; do not use as primary analytic support
[033, 2026]	The Counterintelligence Threat from Non-State Actors	How seriously is the U.S. Intelligence Community (IC) considering this challenge to U.S.	original source-guide context; do not use as primary analytic support
[019, 2026]	Espionage in Our AI Future: Why Human Intelligence Still Matters - CSI	By Thomas Mulligan, a researcher at the RAND Corporation who served in CIA during 2008–14.	original source-guide
[034, 2026]	Studies in Intelligence Vol. 70, No. 1 (Extracts, March 2026) - CSI	Thomas Mulligan is a researcher at the RAND Corporation and former CIA officer. Ana P.	original source-guide

Where this sits. This module's overview is Section 11; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

11.3.4 Source Protection and CI Integration governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 11; [238, 2026].

11.3.5 Source Protection and CI Integration analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 6's governance-boundary section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **Collection Management and Multi-INT Requirements Discipline** for **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**. [238, 2026]; [241, 2026].

Curriculum topic spine: Identifying Penetration: Signs of Compromise, **Compartmentation and need-to-know governance**, **Lie Detection, Vetting, Polygraph, and Its Alternatives**. **Verified anchor cluster:** [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]; [Archives and Administration, 1981]; [Agency, 2026g]; [of the Director of National Intelligence, 2026d].

Conceptual depth: requirements-driven, authority-bounded collection where priorities, legal basis, minimization, source protection, and evaluation are explicit.

Method stack: priority mapping, requirement decomposition, source-discipline fit, coverage-gap review, legal-authority check, and collection-feedback loop.

Composability contract: requirements, authorities, source disciplines, collection notes, retention limits, caveats, and evaluation metrics remain separable.

Known failure modes: opportunistic collection, priority drift, over-collection, weak minimization, source exposure, and confusing availability with authority.

Defensive boundary: collection material remains doctrinal and governance-oriented; it does not teach recruitment, interception, surveillance, or tasking procedures. Applied to **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**.

Anchor	Why it matters here
[Community, 2026]	Official public explanation of the intelligence cycle, collection disciplines, dissemination, evaluation, oversight, and partners. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026c]	Official prioritization directive for translating national intelligence priorities into collection, analysis, risk management, and responsiveness evaluation. Checked as of 2026-05-21; role: curriculum_anchor.
[of Staff, 2026]	Official joint-doctrine landing page for the keystone publication on joint intelligence principles, products, services, and assessments. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence and Agency, 2024]	Official IC OSINT strategy for professionalizing OSINT, integrated collection management, open-source sharing, innovation, and tradecraft. Checked as of 2026-05-21; role: curriculum_anchor.
[Archives and Administration, 1981]	Official legal anchor for intelligence authorities, rights-aware collection, analytic competition, oversight, and source-method protection. Checked as of 2026-05-21; role: curriculum_anchor.
[Agency, 2026g]	Official NSA public explanation of FISA oversight for signals intelligence collection governed by statutory and court-authorized controls. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026d]	Official sourcing directive for traceability, citations, source descriptors, and source summaries. Checked as of 2026-05-21; role: curriculum_anchor.

11.3.5.1 Source Protection and CI Integration evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **Collection Management and Multi-INT Requirements Discipline** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [238, 2026]; [241, 2026].

11.3.6 Source Protection and CI Integration agentic boundary: assist, approve, block, and record

Evidence anchor. Section 11; [238, 2026].

AGEINT translation is bounded by the **Collection Management and Multi-INT Requirements Discipline** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**.

11.3.6.1 Source Protection and CI Integration permitted defensive utility: curriculum uses and safe outputs

Evidence anchor. Section 11; [238, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**.

11.3.6.2 Source Protection and CI Integration excluded operational boundary: blocked actions and stop rules

Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [238, 2026]; [241, 2026] and **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

11.3.7 Source Protection and CI Integration governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 11; [238, 2026].

Governance is practiced as a gate on the **Collection Management and Multi-INT Requirements Discipline** lane. Learners use the **Requirements-to-Evidence Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues

remain, and when an agent-assisted artifact must stop for human review while using **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**.

11.3.7.1 Source Protection and CI Integration governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [238, 2026]; [241, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Collection Management and Multi-INT Requirements Discipline** failure modes and the **Requirements-to-Evidence Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

11.3.7.2 Source Protection and CI Integration evidence package handoff: appendices, records, and reuse

Evidence anchor. Section 11; [238, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Requirements-to-Evidence Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**.

11.3.7.3 Source Protection and CI Integration current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**. [238, 2026]; [241, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_intelligence_gov_how_ic_works` for **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**?	How the IC Works; lane `governed_intelligence_cycle`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official public explanation of the intelligence cycle, collection disciplines, dissemination, evaluation, oversight, and partners.
What does the module inherit from `official_odni_icd_204` for **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**?	Intelligence Community Directive 204: National Intelligence Priorities Framework; lane `collection_management`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official prioritization directive for translating national intelligence priorities into collection, analysis, risk management, and responsiveness evaluation.
What does the module inherit from `official_joint_pub_2_0` for **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**?	JP 2-0: Joint Intelligence; lane `collection_management`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official joint-doctrine landing page for the keystone publication on joint intelligence principles, products, services, and assessments.
What does the module inherit from `official_ic_osint_strategy` for **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**?	The INT of First Resort: The IC OSINT Strategy 2024-2026; lane `osint_geoint`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official IC OSINT strategy for professionalizing OSINT, integrated collection management, open-source sharing, innovation, and tradecraft.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 11; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

11.3.8 Source Protection and CI Integration assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 11; [238, 2026].

11.3.9 Source Protection and CI Integration assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 11; [238, 2026].

11.3.9.1 Source Protection and CI Integration capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance** and [238, 2026]; [241, 2026].

11.3.9.2 Source Protection and CI Integration instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance** and [238, 2026]; [241, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

11.3.9.3 Source Protection and CI Integration assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Identifying Penetration: Signs of Compromise	Completed **requirements matrix with source descriptors, caveats, and collection limits** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Compartmentation and need-to-know governance	Completed **requirements matrix with source descriptors, caveats, and collection limits** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Lie Detection, Vetting, Polygraph, and Its Alternatives	Completed **requirements matrix with source descriptors, caveats, and collection limits** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

11.3.10 Source Protection and CI Integration refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [238, 2026]; [241, 2026] and **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**.

11.3.10.1 Source Protection and CI Integration refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**. The local signals begin with [238, 2026]; [241, 2026].

11.3.10.2 Source Protection and CI Integration claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**, and the source spine for these checks begins with [238, 2026]; [241, 2026].

11.3.11 Source Protection and CI Integration reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [238, 2026]; [241, 2026].

Triangulation anchors. In module 6's review-checklist section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance**. [238, 2026]; [241, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

11.3.12 Source Protection and CI Integration learning-path links: module map, overview, and curriculum atlas

Follow the cross-links to move between **Identifying Penetration: Signs of Compromise; Compartmentation and need-to-know governance** and the rest of the curriculum without losing the source spine: orientation first, then the parent unit, then the modules on either side. Primary sources: [238, 2026]; [241, 2026].

Section 2, Section 8, Section 10, Section 12

12 SIGNALS INTELLIGENCE (SIGINT)

12.1 SIGNALS INTELLIGENCE (SIGINT) learning spine and source route: unit purpose, module order, and evidence handoff

Evidence anchor. Section 12; [255, 2026].

12.1.1 signals-intelligence governance discipline spine: domain question and learning focus

Evidence anchor. Section 12; [255, 2026].
This unit teaches **signals-intelligence governance**. SIGINT is taught as legal, technical, and minimization-aware interpretation of signal-derived evidence, not interception procedure.

12.1.2 signals-intelligence governance source-use contract: citation roles and evidence limits

Evidence anchor. Section 12; [255, 2026].
Use source-guide citations for discipline concepts and directive/legal anchors for authority, minimization, retention, and dissemination claims.

12.1.3 signals-intelligence governance practice artifact: recurring packet and retained evidence

Evidence anchor. Section 12; [255, 2026].
The recurring practice artifact is a **signal-evidence minimization card** that draws on authority boundary note, minimization field, signal-quality caveat, and dissemination restriction. The unit keeps its learning spine explicit. Learners separate signal availability, collection authority, analytic inference, and dissemination controls.

12.1.4 signals-intelligence governance safety boundary: accountable, synthetic, and evidence-bounded limits

No interception, decryption, surveillance target selection, or collection-expansion guidance.
This unit introduces the part's governing question, evidence artifacts, source-support spine, and capstone thread before the individual modules begin. [255, 2026]; [258, 2026].
Learners carry one unit capstone thread through the part: define an accountable intelligence question, bind it to source-quality constraints, produce a reviewable artifact, test the artifact against failure modes, and hand it off with enough context for another analyst or instructor to audit. The capstone remains public, synthetic, or owned-lab throughout; its first source anchors are [255, 2026]; [258, 2026].
This unit's deliverables are a source-canon card, claim/evidence ledger, safe-practice lab packet, failure-mode note, instructor rubric, and debrief memo. The full source-lane and evidence-package ledgers appear in the orientation and appendices; this unit introduction keeps only the learner-facing spine for [255, 2026]; [258, 2026].
This unit's safety gates are scope authorization, rights review, data provenance, tool allowlisting, human oversight, rollback, and evidence-bounded output. A missing gate turns the activity into a tabletop, audit, or written governance exercise until the gate is restored against [255, 2026]; [258, 2026].
Capstone thread:

Phase	Artifact	Review gate
Question	accountable learning question and excluded-action list	instructor confirms scope, allowed data, and rights impact
Source canon	source-lane map with guide citations, verified anchors, and refresh dates	citation keys resolve and source identity lock remains stable
Evidence ledger	claim, evidence, uncertainty, confidence, and reviewer register	every material claim has a source, caveat, and owner
Safe lab	synthetic or public dataset packet, tool allowlist, and stop conditions	no live target, private data, external action, or unsafe cyber-physical step
Assurance	evaluation rubric, failure-mode drill, rights map, and remediation note	human reviewer signs off before presentation or reuse
Debrief	capstone memo with lessons, residual risk, refresh triggers, and handoff owner	all unresolved questions and future approvals are explicit

Research lane: Collection Management and Multi-INT Requirements Discipline. Core anchors: [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]. Conceptual focus: requirements-driven, authority-bounded collection where priorities, legal basis, minimization, source protection, and evaluation are explicit. Composability contract: requirements, authorities, source disciplines, collection notes, retention limits, caveats, and evaluation metrics remain separable. **Practice lens:** Requirements-to-Evidence Lens; What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit? [255, 2026]; [258, 2026].

12.1.5 SIGNALS INTELLIGENCE (SIGINT) visual navigation and module map: evidence flow, order, and safety cues

The unit uses Figure 41 and Figure 42 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 11, Section 13.

12.1.6 SIGNALS INTELLIGENCE (SIGINT) module roster and source-lane inventory: citations, lanes, and learner route

Module	Section reference	Source spine
SIGINT Fundamentals	Section 13	[255, 2026]; [258, 2026]; [261, 2026]; [279, 2026]; [282, 2026]; [284, 2026]; [289, 2026]; [291, 2026]; [296, 2026]; [035, 2026]; [036, 2026]; [037, 2026]; [038, 2026]; [039, 2026]; [040, 2026].
Modern SIGINT and Cryptography	Section 14	[258, 2026]; [260, 2026]; [261, 2026]; [275, 2026]; [276, 2026]; [283, 2026]; [286, 2026]; [293, 2026]; [295, 2026]; [041, 2026]; [042, 2026]; [027, 2026]; [028, 2026]; [043, 2026]; [044, 2026]; [045, 2026]; [046, 2026]; [018, 2026]; [298, 2026]; [297, 2026]; [309, 2026]; [310, 2026]; [300, 2026].

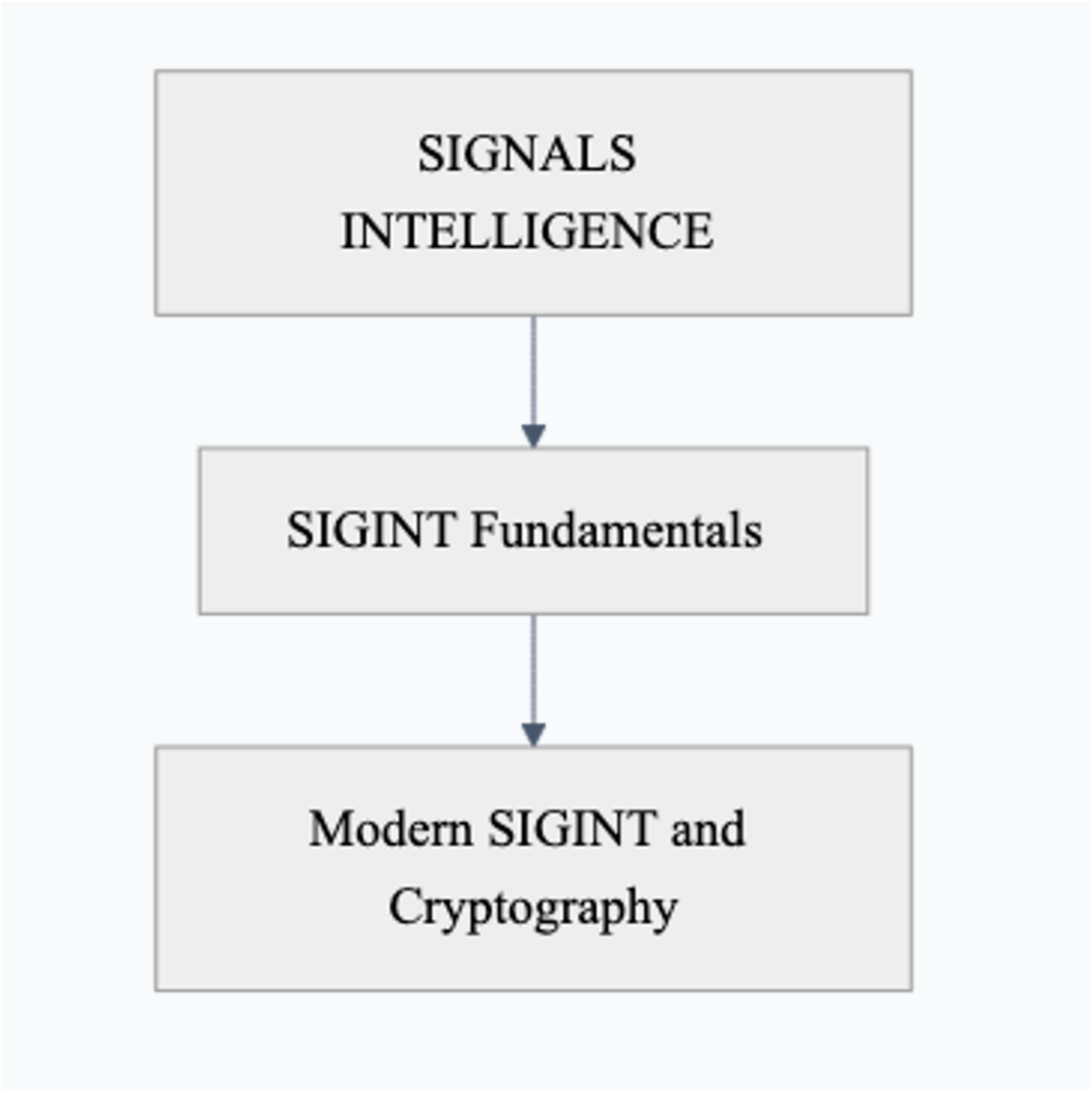


Figure 41: The unit module map traces the part's chapters as a linear reading sequence. Its reader value is to make 2 module nodes in the unit's ordered, source-backed reading sequence from its first module to its last visible at a glance, with the signals intelligence sigint section as the source section and defensive review as the boundary.

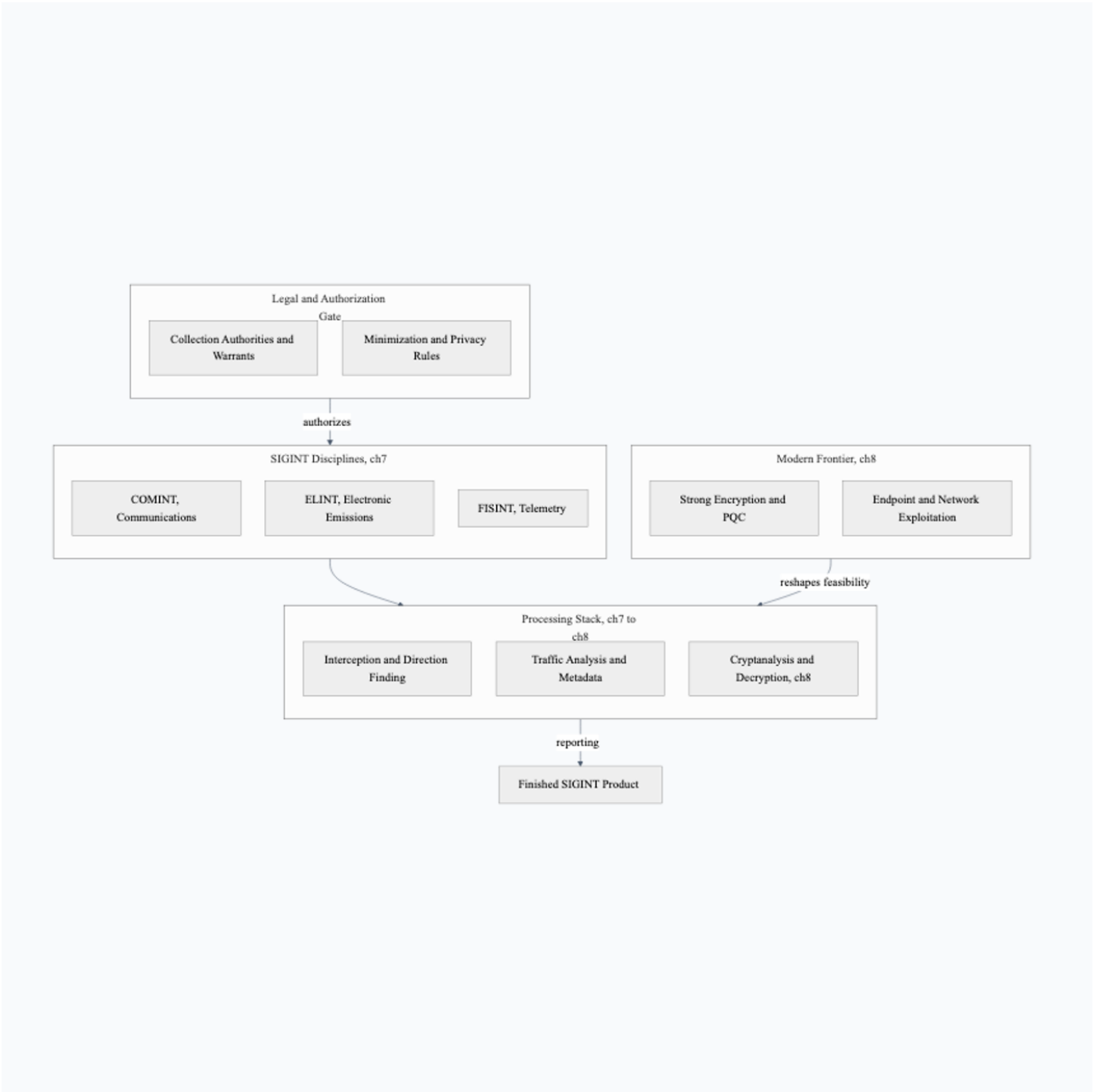


Figure 42: Part III shows SIGINT as a legally gated, layered pipeline where authorities and minimization rules govern collection disciplines (ch7), feed a processing stack into cryptanalysis (ch8), with the modern crypto frontier reshaping what is feasible. In the signals intelligence sigint section, it lets readers compare Legal and Authorization Gate, Collection Authorities and Warrants, Minimization and Privacy Rules, and SIGINT Disciplines, ch7 so the visual functions as a traceable course aid rather than an unscoped assertion.

13 SIGINT Fundamentals

13.0.1 SIGINT Fundamentals figures and course links: visual evidence, source flow, and navigation

The module uses Figure 43 and Figure 41 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 12, Section 14.
This module teaches the **Collection Management and Multi-INT Requirements Discipline** lane through a bounded, source-backed coursebook chapter. [255, 2026]; [258, 2026].

13.1 Collection Management and Multi-INT Requirements Discipline frame for SIGINT Fundamentals: source context, topic focus, and reader task

Evidence anchor. Section 13; [255, 2026].

13.1.1 SIGINT Fundamentals orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 13; [255, 2026].

13.1.2 SIGINT Fundamentals conceptual primer: source context, core model, and reader task

This chapter teaches collection management as requirements discipline: a source method is considered only after the priority, authority, minimization rule, source risk, and evaluation plan are explicit. The chapter uses **Requirements-to-Evidence Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**.
The central distinction is to separate collection discipline concepts from operational recruitment, interception, or tasking procedures. Core topics include **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise; Spartans in Darkness: SIGINT legal-authority and communications-security governance exercise**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [255, 2026]; [258, 2026].
Learners move from vocabulary and the **Requirements-to-Evidence Lens** distinction through topic lessons on **SIGINT legal-authority and communications-security governance exercise** with evidence and misconception checks, then assemble a **requirements matrix with source descriptors, caveats, and collection limits** with safety and rights gates.

13.1.3 SIGINT Fundamentals learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 13; [255, 2026].

- Connect **SIGINT legal-authority and communications-security governance exercise and WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise** to **Collection Management and Multi-INT Requirements Discipline** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **requirements matrix with source descriptors, caveats, and collection limits** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate collection discipline concepts from operational recruitment, interception, or tasking procedures; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as opportunistic collection, priority drift, over-collection, weak minimization, source exposure, and confusing availability with authority, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: collection material remains doctrinal and governance-oriented; it does not teach recruitment, interception, surveillance, or tasking procedures.

13.1.4 SIGINT Fundamentals core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 13; [255, 2026].

Term	Working definition
Priority	the relative importance of an intelligence question
Source discipline	a broad evidence channel such as HUMINT, SIGINT, GEOINT, OSINT, or FININT
Minimization	the rule that limits acquisition, retention, or use of unnecessary information
Source protection	the duty to reduce risk to people, methods, and sensitive relationships
Evaluation	the feedback step that tests whether the evidence satisfied the requirement
Gray-zone indicator	an observable signal of ambiguous coercion below armed conflict thresholds
Proxy pattern	a relationship suggesting indirect sponsorship without confirmed operational control
SIGINT legal-authority and…	Key terms: SIGINT, legal, authority.
WWII Axis SIGINT: SIGINT legal-authority and…	Key terms: WWII, Axis, SIGINT.

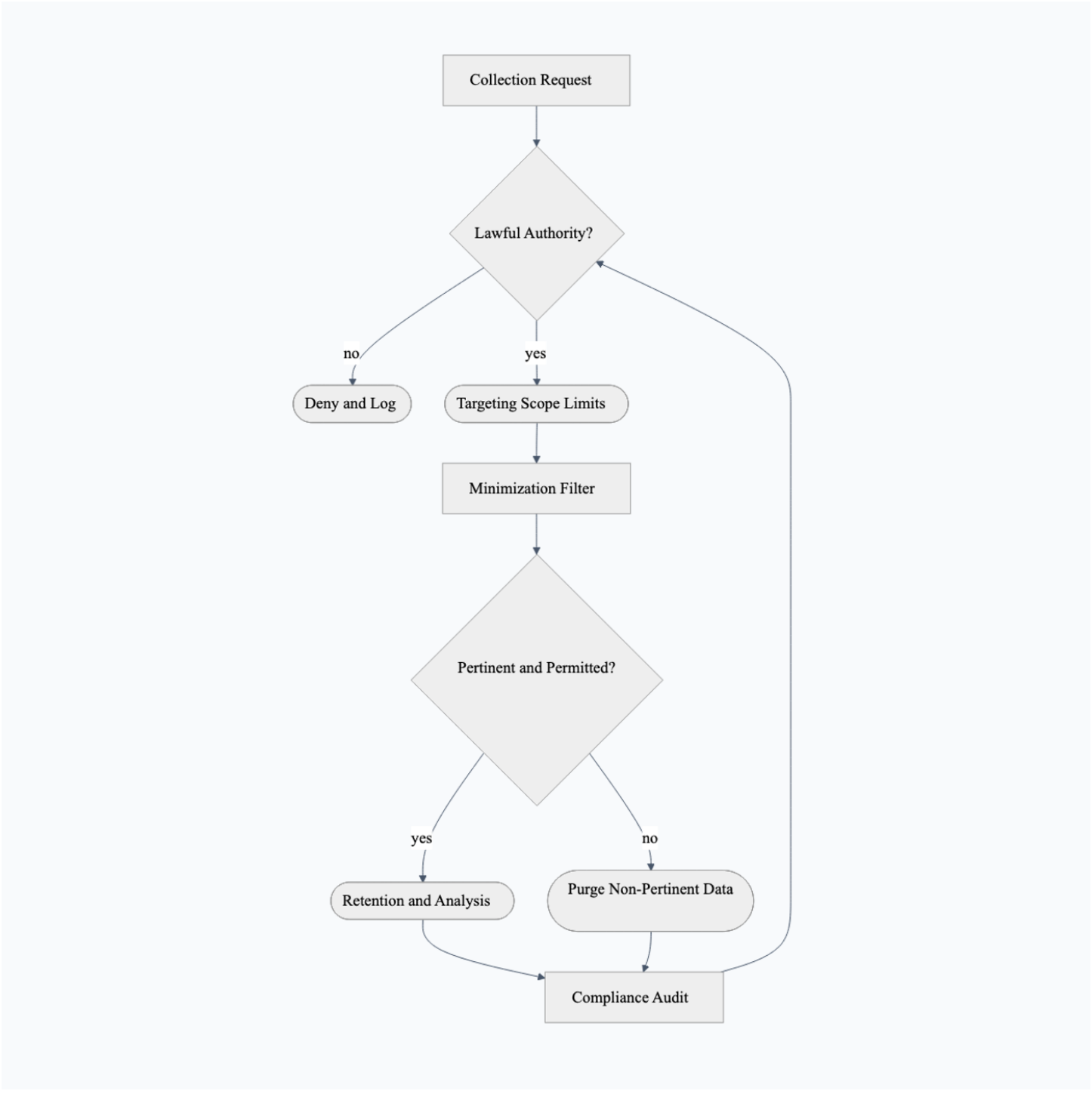


Figure 43: This diagram teaches how a lawful-authority check and minimization rules gate signals collection so that non-pertinent and protected data are filtered before retention. It is anchored to the signals intelligence sigint / sigint fundamentals section; use it to inspect Collection Request, Minimization Filter, and Compliance Audit while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

13.2 Requirements-to-Evidence Lens path for SIGINT Fundamentals: lesson cluster, safe artifact, and review

Evidence anchor. Section 13; [255, 2026].

13.2.1 SIGINT Fundamentals practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 13; [255, 2026].

13.2.2 SIGINT Fundamentals topic lessons: source-backed concepts and transfer tasks

This module builds collection management as requirements discipline: a source method is considered only after the priority, authority, minimization rule, source risk, and evaluation plan are explicit. The sequence opens with **SIGINT legal-authority and communications-security governance exercise**, **WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**, **Spartans in Darkness: SIGINT legal-authority and communications-security governance exercise** and applies the **Requirements-to-Evidence Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 41; module overview Section 13; curriculum atlas Section 2.

Triangulation anchors. In module 7's topic-lessons section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

13.2.2.1 Lesson 1: SIGINT legal-authority and communications-security governance exercise

Concept. SIGINT legal-authority and communications-security governance exercise distinguishes communications content from electronic signatures by evidence type, authority, minimization, and uncertainty.

Why it matters. Without explicit treatment of **SIGINT legal-authority**, opportunistic collection undermines requirements decomposition and source-discipline fit review; the lesson builds the habit to separate collection discipline concepts from operational recruitment, interception, or tasking procedures.

Source support. SIGINT legal-authority and communications-security governance exercise rests on [035, 2026]. The closest source to this row notes: SIGINT is intelligence derived from electronic signals and systems used by foreign targets. Use it for pinning down the scope of **SIGINT legal-authority and communications-security governance exercise**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. Read **SIGINT legal-authority** against the works cited for this row. [035, 2026] SIGINT is intelligence derived from electronic signals and systems used by foreign targets. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **SIGINT legal-authority**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must state the authority descriptor, the bounded claim about **SIGINT legal-authority and communications-security governance**, the minimization caveat, the uncertainty note, the collection boundary, and the reviewer accountable for the authorization. Shape **SIGINT legal-authority** work as a **signal-evidence minimization card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **SIGINT legal-authority**: that a named collection authority removes the minimization and retention limits on what may be kept.

Transfer task. Reuse the **SIGINT legal-authority** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

13.2.2.2 Lesson 2: WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise

Concept. WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise frames SIGINT as authority-bound collection with minimization, handling rules, and communications-security implications.

Why it matters. Analysts use **WWII Axis SIGINT** to separate collection discipline concepts from operational recruitment, interception, or tasking procedures. A defensible treatment names the judgment it enables for requirements decomposition and source-discipline fit review, the proof limit that opportunistic collection would otherwise hide, and the reviewer accountable for challenge.

Source support. WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise rests on [036, 2026]. The closest source to this row notes: Volumes 1 - 9 of the European Axis Signal Intelligence in WWII documentation. Use it for pinning down the scope of **WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. Ground **WWII Axis SIGINT** in the evidence the row cites. [036, 2026] Volumes 1 - 9 of the European Axis Signal Intelligence in WWII documentation. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **WWII Axis SIGINT**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must state the authority descriptor, the bounded claim about **WWII Axis SIGINT**, the minimization caveat, the uncertainty note, the collection boundary, and the reviewer accountable for the authorization. Shape **WWII Axis SIGINT** work as a **signal-evidence minimization card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **WWII Axis SIGINT**: that a named collection authority removes the minimization and retention limits on what may be kept.

Transfer task. Apply this module's safe boundary for **WWII Axis SIGINT** to another artifact while keeping requirements decomposition and source-discipline fit and reviewer ownership explicit.

13.2.2.3 Lesson 3: Spartans in Darkness: SIGINT legal-authority and communications-security governance exercise

Concept. Spartans in Darkness: SIGINT legal-authority and communications-security governance exercise frames SIGINT as authority-bound collection with minimization, handling rules, and communications-security implications.

Why it matters. Without explicit treatment of **Spartans in Darkness**, opportunistic collection undermines requirements decomposition and source-discipline fit review; the lesson builds the habit to separate collection discipline concepts from operational recruitment, interception, or tasking procedures.

Source support. Spartans in Darkness: SIGINT legal-authority and communications-security governance exercise rests on [037, 2026]. The lead source's own note reads: This Federation of American Scientists article reports on the NSA's declassification of a roughly 500-page historical study titled "Spartans in Darkness," which examines American signals intelligence during the Vietnam War from 1945 to 1975. Use it for the working definition that **Spartans in Darkness: SIGINT legal-authority and communications-security governance exercise** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. For **Spartans in Darkness**, work from the cited evidence behind this row. [037, 2026] This Federation of American Scientists article reports on the NSA's declassification of a roughly 500-page historical study titled "Spartans in Darkness," which examines American signals intelligence during the Vietnam War from 1945 to 1975. Author Robert J. Hanyok documents that no second attack occurred during the 1964 Gulf of Tonkin Incident, contradicting prior official testimony, and also covers episodes such as the Tet Offensive and the Son Tay prison rescue. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Spartans in Darkness**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must state the authority descriptor, the bounded claim about **Spartans in Darkness**, the minimization caveat, the uncertainty note, the collection boundary, and the reviewer accountable for the authorization. Shape **Spartans in Darkness** work as a **signal-evidence minimization card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Spartans in Darkness**: that a named collection authority removes the minimization and retention limits on what may be kept.

Transfer task. Transfer **Spartans in Darkness** from this module to a second motif by preserving requirements decomposition and source-discipline fit, replacing action with audit, and naming the blocked use.

13.2.2.4 Lesson 4: CIA NSA SIGINT Relationship: SIGINT legal-authority and communications-security governance exercise

Concept. CIA NSA SIGINT Relationship: SIGINT legal-authority and communications-security governance exercise frames SIGINT as authority-bound collection with minimization, handling rules, and communications-security implications.

Why it matters. CIA NSA SIGINT Relationship matters in the **Collection Management and Multi-INT Requirements Discipline** lane because requirements decomposition and source-discipline fit evidence must stay separate from judgment; opportunistic collection is a common failure.

Source support. CIA NSA SIGINT Relationship: SIGINT legal-authority and communications-security governance exercise rests on [038, 2026] and [039, 2026]. The closest source to this row notes: Richelson, presenting declassified documents on the CIA's signals intelligence activities from roughly 1947 to 1970. Use them for fixing what **CIA NSA SIGINT Relationship: SIGINT legal-authority and communications-security governance exercise** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. For **CIA NSA SIGINT Relationship**, reason from the sources cited in this row. [038, 2026] A January 2018 blog post on Open INT recounting the CIA's role in signals intelligence from roughly 1947 to 1970, noting that SIGINT is often associated with the NSA but the CIA also participated. It distinguishes communications intelligence from electronic intelligence and references declassified Cold War operations including U-2 collection and a Berlin communications-tapping effort. [039, 2026] A 2015 briefing book from the National Security Archive, compiled by Jeffrey T. Richelson, presenting declassified documents on the CIA's signals intelligence activities from roughly 1947 to 1970. It documents the CIA's parallel SIGINT operations alongside the NSA during the Cold War, covering programs and collection efforts as well as recurring friction between the two agencies over mission overlap, budgets, and access to intelligence. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **CIA NSA SIGINT Relationship**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must state the authority descriptor, the bounded claim about **CIA NSA SIGINT Relationship**, the minimization caveat, the uncertainty note, the collection boundary, and the reviewer accountable for the authorization. Shape **CIA NSA SIGINT Relationship** work as a **signal-evidence minimization card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **CIA NSA SIGINT Relationship**: that a named collection authority removes the minimization and retention limits on what may be kept.

Transfer task. Reuse the **CIA NSA SIGINT Relationship** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

13.2.2.5 Lesson 5: NSA Basic Cryptography: SIGINT legal-authority and communications-security governance exercise

Concept. NSA Basic Cryptography: SIGINT legal-authority and communications-security governance exercise frames SIGINT as authority-bound collection with minimization, handling rules, and communications-security implications.

Why it matters. NSA Basic Cryptography matters in the **Collection Management and Multi-INT Requirements Discipline** lane because requirements decomposition and source-discipline fit evidence must stay separate from judgment; opportunistic collection is a common failure.

Source support. NSA Basic Cryptography: SIGINT legal-authority and communications-security governance exercise rests on [040, 2026]. The most specific cited work observes: Codes will first be considered, but as they do not fulfill the conditions required of a means. Use it for fixing what **NSA Basic Cryptography: SIGINT legal-authority and communications-security governance exercise** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. Read **NSA Basic Cryptography** against the works cited for this row. [040, 2026] Codes will first be considered, but as they do not fulfill the conditions required of a means. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **NSA Basic Cryptography**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must state the authority descriptor, the bounded claim about **NSA Basic Cryptography**, the minimization caveat, the uncertainty note, the collection boundary, and the reviewer accountable for the authorization. Shape **NSA Basic Cryptography** work as a **signal-evidence minimization card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **NSA Basic Cryptography**: that a named collection authority removes the minimization and retention limits on what may be kept.

Transfer task. Apply this module's safe boundary for **NSA Basic Cryptography** to another artifact while keeping requirements decomposition and source-discipline fit and reviewer ownership explicit.

13.2.3 SIGINT Fundamentals worked safe example: synthetic inputs, evidence, and review

Worked example: a synthetic policy cell compares public indicators of hybrid pressure against an approved collection plan for a benign border-disruption exercise. [255, 2026]; [258, 2026].

Triangulation anchors. In module 7's worked-example section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **signals-intelligence governance**. Learners use a **signal-evidence minimization card** and keep this boundary visible: No interception, decryption, surveillance target selection, or collection-expansion guidance.

Frame. The classroom question centers on **SIGINT legal-authority and communications-security governance exercise**. Excluded actions

stay explicit, and the **Requirements-to-Evidence Lens** planning question is: What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit?

Inputs. For the **SIGINT legal-authority and communications-security governance exercise** scenario, use public notices, synthetic interview summaries, public logistics records, and an instructor scope card. The Requirements-to-Evidence Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **SIGINT legal-authority and communications-security governance exercise**, students rank requirements, choose the least intrusive source discipline, list excluded actions, and evaluate evidence quality. Pause whenever an inference about SIGINT legal-authority and communications-security governance exercise appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **SIGINT legal-authority and communications-security governance exercise** classroom scenario; unit artifact = signal-evidence minimization card; evidence = allowed inputs; method = requirements decomposition and source-discipline fit; output = a requirements-to-evidence matrix with discipline fit, source caveats, minimization notes, and gaps; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **SIGINT legal-authority and communications-security governance exercise** as "Requirements-to-Evidence Lens confirms it" is not enough. The revision ties the claim to requirements decomposition and source-discipline fit, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **SIGINT legal-authority and communications-security governance exercise** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

13.2.4 SIGINT Fundamentals practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Requirements-to-Evidence Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**.

Triangulation anchors. In module 7's practice-sequence section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare SIGINT legal-authority and communications-security governance exercise, WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise, Spartans in Darkness: SIGINT legal-authority and communications-security governance exercise; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Collection Management and Multi-INT Requirements Discipline** lane.
2. Frame	Answer the lens question: What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for SIGINT legal-authority and communications-security governance exercise: requirements matrix with source descriptors, caveats, and collection limits.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the signal-evidence minimization card fields for SIGINT legal-authority and communications-security governance exercise.	Unit profile note.	Evidence artifacts include authority boundary note, minimization field.
4. Challenge	Test the misconception that a named collection authority removes the minimization and retention limits on what may be kept.	Failure-mode note.	The artifact applies the key distinction: separate collection discipline concepts from operational recruitment, interception, or tasking procedures.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

13.2.4.1 SIGINT Fundamentals instructor notes: source reasoning, review points, and studio focus

Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**. [255, 2026]; [258, 2026].

13.2.4.2 SIGINT Fundamentals extension exercise: peer validation and refresh trigger review

Evidence anchor. Section 13; [255, 2026].

Have learners swap artifacts and apply the **Requirements-to-Evidence Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**.

13.2.5 SIGINT Fundamentals knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 13; [255, 2026].

1. Explain how **SIGINT legal-authority and communications-security governance exercise** is defined here; name the source descriptor that supports the definition.

2. Contrast **SIGINT legal-authority and communications-security governance exercise** with **WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise** using the **Requirements-to-Evidence Lens** artifact fields.
3. Identify one failure mode from the **Collection Management and Multi-INT Requirements Discipline** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which gray-zone indicator changes the least-intrusive source choice without crossing into operational tasking?
5. Correct this misconception: that a named collection authority removes the minimization and retention limits on what may be kept.

13.2.5.1 SIGINT Fundamentals answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **SIGINT legal-authority and communications-security governance exercise** without source evidence, uncertainty, or a safe transfer task.

13.3 SIGINT Fundamentals assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 13; [255, 2026].

13.3.1 SIGINT Fundamentals evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 13; [255, 2026].

13.3.2 SIGINT Fundamentals transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 13; [255, 2026].

13.3.2.1 SIGINT Fundamentals lineage and source tradition: profile, concepts, and first anchors This sits in the **Collection Management and Multi-INT Requirements Discipline** lineage: requirements-driven, authority-bounded collection where priorities, legal basis, minimization, source protection, and evaluation are explicit. [255, 2026]; [258, 2026].

13.3.2.2 SIGINT Fundamentals working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 13; [255, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**, with provenance and reviewability throughout.

13.3.2.3 SIGINT Fundamentals knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** accountable requirements, source-discipline choices, minimization rules, source-risk notes, and evaluation criteria. [255, 2026]; [258, 2026].
- **Transforms:** priority mapping, source-discipline fit, least-intrusive evidence selection, and feedback review.
- **Outputs:** requirements matrix, collection-limit note, source-quality card, and gap list.
- **Failure modes:** recruitment or interception drift, over-collection, weak minimization, and source exposure.

13.3.2.4 SIGINT Fundamentals transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 13; [255, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**.
- **Evidence contract:** keep the **Collection Management and Multi-INT Requirements Discipline** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as requirements matrix, collection-limit note, source-quality card, and gap list that another reviewer can audit.

13.3.2.5 SIGINT Fundamentals profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 13; [255, 2026].

The matched profile emphasizes requirements-driven, authority-bounded collection where priorities, legal basis, minimization, source protection, and evaluation are explicit. The method stack is priority mapping, requirement decomposition, source-discipline fit, coverage-gap review, legal-authority check, and collection-feedback loop; the local topic cluster is **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**.

13.3.3 SIGINT Fundamentals evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 13; [255, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Collection Management and Multi-INT Requirements Discipline** profile tells reviewers what evidence is strong enough for the module artifact built around **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**.

13.3.3.1 SIGINT Fundamentals guide source spine: inherited keys and local citation roles Primary guide citations: [255, 2026]; [258, 2026]; [261, 2026]; [279, 2026]; [282, 2026]; [284, 2026]; [289, 2026]; [291, 2026]; [296, 2026]; [035, 2026]; [036, 2026]; [037, 2026]; [038, 2026]; [039, 2026]; [040, 2026].

13.3.3.2 SIGINT Fundamentals verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [255, 2026]; [258, 2026].

Tier	What counts	How it is used
Source guide	[255, 2026]; [258, 2026]; [261, 2026]; [279, 2026]; [282, 2026]; [284, 2026]; [289, 2026]; [291, 2026]; [296, 2026]; [035, 2026]; [036, 2026]; [037, 2026]; [038, 2026]; [039, 2026]; [040, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 7's source-canon section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise** and [255, 2026]; [258, 2026], but only directly verified source URLs are encoded as citations.

13.3.3.3 SIGINT Fundamentals intelligence practice lens: evidence artifact and safety check Practice lens: **Requirements-to-Evidence Lens** for **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**. [255, 2026]; [258, 2026].

Planning question: What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit?

Evidence artifact: requirements matrix with source descriptors, caveats, and collection limits.

Validation rule: show priority, authority, minimization, corroboration, and source quality before any claim is reused. Applied to **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**.

Handoff contract: deliver metadata-rich evidence packets, not unscoped data piles or implicit targeting requests.

Safety check: exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure.

13.3.3.4 SIGINT Fundamentals runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 13; [255, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	7.99	7.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind SIGINT Fundamentals to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Bounded autonomy, procurement, incident-response, and assurance studio	7.101	7.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for SIGINT Fundamentals	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Model-card, recoverability, retention, and learner-support evidence package	7.102	7.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for SIGINT Fundamentals	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
SIGINT legal-authority and communications-security governance exercise	7.1	7.1 source title transformed into safe curriculum treatment; original: COMINT and ELINT: Definitions and Distinctions	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
SIGINT legal-authority and communications-security governance exercise	7.2	7.2 source title transformed into safe curriculum treatment; original: Historical Foundations: WWII Axis SIGINT (NSA Declassified 9 Volumes)	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
SIGINT legal-authority and communications-security governance exercise	7.3	7.3 source title transformed into safe curriculum treatment; original: Spartans in Darkness: SIGINT in the Indochina War, 1945–1975	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
SIGINT legal-authority and communications-security governance exercise	7.4	7.4 source title transformed into safe curriculum treatment; original: CIA–NSA SIGINT Relationship, 1947–1970	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
SIGINT legal-authority and communications-security governance exercise	7.5	7.5 source title transformed into safe curriculum treatment; original: NSA Basic Cryptography (Friedman Documents)	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought

13.3.3.5 SIGINT Fundamentals reusable subsection contract: topic rows, artifacts, and safety duties **Evidence anchor.** Section 13; [255, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
SIGINT legal-authority and communications-security governance exercise	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
Spartans in Darkness: SIGINT legal-authority and communications-security governance exercise	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
CIA NSA SIGINT Relationship: SIGINT legal-authority and communications-security governance exercise	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
NSA Basic Cryptography: SIGINT legal-authority and communications-security governance exercise	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought

13.3.3.6 SIGINT Fundamentals annotated source ledger: real titles and local contribution Each source cited by this **Collection Management and Multi-INT Requirements Discipline** module is paired below with its real title and a one-line note on what it contributes to **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**.

Source	Cited work	What it contributes	Status
[255, 2026]	Web of Things (WoT) Architecture 1.1	The W3C Recommendation for Web of Things Architecture 1.1, published in December 2023, defining an abstract architecture for interoperability across diverse Internet of Things platforms. It introduces core concepts including Things described by machine-readable Thing Descriptions, reusable Thing Models, and Consumers that interpret descriptions to interact via Properties, Actions, and Events.	verified source-guide

Source	Cited work	What it contributes	Status
[258, 2026]	OpenAPI Specification	The official OpenAPI Initiative publications page, serving as a central index for the OpenAPI Specification and related standards including the Arazzo and Overlay specifications. It provides access to multiple specification versions (2.0, 3.0, 3.1, and 3.2) and their corresponding downloadable schemas identified by release date, along with a registry of extensions, formats, media types, and other resources.	verified source-guide
[261, 2026]	RFC 9110: HTTP Semantics	RFC 9110, the official IETF standards document defining the core semantics and architecture of HTTP, published in June 2022 and consolidating nine earlier RFCs. It establishes terminology and protocol aspects shared across HTTP versions, including methods, status codes, header fields, content negotiation, conditional and range requests, authentication, and the http and https URI schemes.	verified source-guide
[279, 2026]	Open Contracting Data Standard	The documentation homepage for the Open Contracting Data Standard, version 1.1.5, maintained by the Open Contracting Partnership to support disclosure of government contracting data across the procurement lifecycle. It provides a common data model spanning planning, tender, award, contract, and implementation stages, along with a primer, implementation guidance, technical schemas, and validation tooling.	verified source-guide
[282, 2026]	AI Research: Security and Resilience	A NIST page on AI research focused on security and resilience, framing these as core characteristics of trustworthy AI under the NIST AI Risk Management Framework.	verified source-guide
[284, 2026]	Verifiable Credential Data Integrity 1.0	The W3C Recommendation for Verifiable Credential Data Integrity 1.0, published May 2025, defining mechanisms for ensuring the authenticity and integrity of verifiable credentials using cryptographic proofs. It specifies a process of data transformation, hashing, and proof generation, and a corresponding verification procedure, along with a proof data model containing properties such as type, verification method, purpose, and proof value.	verified source-guide
[289, 2026]	Guidance for Organisations Using the Algorithmic Transparency Recording Standard	This is a GOV.UK guidance page published by the Government Digital Service that instructs public sector organizations on completing the Algorithmic Transparency Recording Standard (ATRS) template and publishing their records to the GOV.UK repository. It applies both to central government bodies required to publish under mandatory policy and to other public sector bodies doing so voluntarily.	verified source-guide

Source	Cited work	What it contributes	Status
[291, 2026]	Revised 508 Standards and 255 Guidelines	Official documentation from the U.S. Access Board on the Revised 508 Standards and 255 Guidelines for information and communication technology accessibility. It establishes mandatory accessibility requirements for federal agencies and voluntary guidelines for telecommunications manufacturers, covering hardware, software, websites, electronic documents, and support services.	verified source-guide
[296, 2026]	Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile	NIST AI 600-1, the Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, a cross-sectoral companion resource to the NIST AI RMF 1.0 issued pursuant to Executive Order 14110. It identifies risks that are unique to or amplified by generative AI and organizes suggested actions for managing those risks, mapped to the AI RMF functions.	verified source-guide
[035, 2026]	Signals Intelligence (SIGINT) Overview	SIGINT is intelligence derived from electronic signals and systems used by foreign targets.	original source-guide
[036, 2026]	European Axis Signal Intelligence in World War II	Volumes 1 - 9 of the European Axis Signal Intelligence in WWII documentation.	original source-guide
[037, 2026]	NSA Releases History of American SIGINT and the Vietnam War	This Federation of American Scientists article reports on the NSA's declassification of a roughly 500-page historical study titled "Spartans in Darkness," which examines American signals intelligence during the Vietnam War from 1945 to 1975. Author Robert J. Hanyok documents that no second attack occurred during the 1964 Gulf of Tonkin Incident, contradicting prior official testimony, and also covers episodes such as the Tet Offensive and the Son Tay prison rescue.	verified source-guide
[038, 2026]	History of signals intelligence at the CIA - Open INT	A January 2018 blog post on Open INT recounting the CIA's role in signals intelligence from roughly 1947 to 1970, noting that SIGINT is often associated with the NSA but the CIA also participated. It distinguishes communications intelligence from electronic intelligence and references declassified Cold War operations including U-2 collection and a Berlin communications-tapping effort.	verified source-guide
[039, 2026]	The CIA and Signals Intelligence / National Security Archive	A 2015 briefing book from the National Security Archive, compiled by Jeffrey T. Richelson, presenting declassified documents on the CIA's signals intelligence activities from roughly 1947 to 1970. It documents the CIA's parallel SIGINT operations alongside the NSA during the Cold War, covering programs and collection efforts as well as recurring friction between the two agencies over mission overlap, budgets, and access to intelligence.	verified source-guide
[040, 2026]	BASIC CRYPTOGRAPHY	Codes will first be considered, but as they do not fulfill the conditions required of a means.	original source-guide

Where this sits. This module's overview is Section 13; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

13.3.4 SIGINT Fundamentals governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 13; [255, 2026].

13.3.5 SIGINT Fundamentals analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 7's governance-boundary section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **Collection Management and Multi-INT Requirements Discipline** for **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**. [255, 2026]; [258, 2026].

Curriculum topic spine: SIGINT legal-authority and communications-security governance exercise, **WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**, **Spartans in Darkness: SIGINT legal-authority and communications-security governance exercise**. **Verified anchor cluster:** [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]; [Archives and Administration, 1981]; [Agency, 2026g]; [of the Director of National Intelligence, 2026d].

Conceptual depth: requirements-driven, authority-bounded collection where priorities, legal basis, minimization, source protection, and evaluation are explicit.

Method stack: priority mapping, requirement decomposition, source-discipline fit, coverage-gap review, legal-authority check, and collection-feedback loop.

Composability contract: requirements, authorities, source disciplines, collection notes, retention limits, caveats, and evaluation metrics remain separable.

Known failure modes: opportunistic collection, priority drift, over-collection, weak minimization, source exposure, and confusing availability with authority.

Defensive boundary: collection material remains doctrinal and governance-oriented; it does not teach recruitment, interception, surveillance, or tasking procedures. Applied to **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**.

Anchor	Why it matters here
[Community, 2026]	Official public explanation of the intelligence cycle, collection disciplines, dissemination, evaluation, oversight, and partners. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026c]	Official prioritization directive for translating national intelligence priorities into collection, analysis, risk management, and responsiveness evaluation. Checked as of 2026-05-21; role: curriculum_anchor.
[of Staff, 2026]	Official joint-doctrine landing page for the keystone publication on joint intelligence principles, products, services, and assessments. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence and Agency, 2024]	Official IC OSINT strategy for professionalizing OSINT, integrated collection management, open-source sharing, innovation, and tradecraft. Checked as of 2026-05-21; role: curriculum_anchor.
[Archives and Administration, 1981]	Official legal anchor for intelligence authorities, rights-aware collection, analytic competition, oversight, and source-method protection. Checked as of 2026-05-21; role: curriculum_anchor.
[Agency, 2026g]	Official NSA public explanation of FISA oversight for signals intelligence collection governed by statutory and court-authorized controls. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026d]	Official sourcing directive for traceability, citations, source descriptors, and source summaries. Checked as of 2026-05-21; role: curriculum_anchor.

13.3.5.1 SIGINT Fundamentals evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **Collection Management and Multi-INT Requirements Discipline** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [255, 2026]; [258, 2026].

13.3.6 SIGINT Fundamentals agentic boundary: assist, approve, block, and record

Evidence anchor. Section 13; [255, 2026].

AGEINT translation is bounded by the **Collection Management and Multi-INT Requirements Discipline** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**.

13.3.6.1 SIGINT Fundamentals permitted defensive utility: curriculum uses and safe outputs

Evidence anchor. Section 13; [255, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**.

13.3.6.2 SIGINT Fundamentals excluded operational boundary: blocked actions and stop rules

Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [255, 2026]; [258, 2026] and **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

13.3.7 SIGINT Fundamentals governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 13; [255, 2026].
Governance is practiced as a gate on the **Collection Management and Multi-INT Requirements Discipline** lane. Learners use the **Requirements-to-Evidence Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**.

13.3.7.1 SIGINT Fundamentals governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [255, 2026]; [258, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Collection Management and Multi-INT Requirements Discipline** failure modes and the **Requirements-to-Evidence Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

13.3.7.2 SIGINT Fundamentals evidence package handoff: appendices, records, and reuse **Evidence anchor.** Section 13; [255, 2026].
Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Requirements-to-Evidence Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**.

13.3.7.3 SIGINT Fundamentals current-source assurance: verified anchors and local artifact fit The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**. [255, 2026]; [258, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_intelligence_gov_how_ic_works` for **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**?	How the IC Works; lane `governed_intelligence_cycle`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official public explanation of the intelligence cycle, collection disciplines, dissemination, evaluation, oversight, and partners.
What does the module inherit from `official_odni_icd_204` for **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**?	Intelligence Community Directive 204: National Intelligence Priorities Framework; lane `collection_management`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official prioritization directive for translating national intelligence priorities into collection, analysis, risk management, and responsiveness evaluation.
What does the module inherit from `official_joint_pub_2_0` for **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**?	JP 2-0: Joint Intelligence; lane `collection_management`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official joint-doctrine landing page for the keystone publication on joint intelligence principles, products, services, and assessments.
What does the module inherit from `official_ic_osint_strategy` for **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**?	The INT of First Resort: The IC OSINT Strategy 2024-2026; lane `osint_geoint`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official IC OSINT strategy for professionalizing OSINT, integrated collection management, open-source sharing, innovation, and tradecraft.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 13; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

13.3.8 SIGINT Fundamentals assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 13; [255, 2026].

13.3.9 SIGINT Fundamentals assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 13; [255, 2026].

13.3.9.1 SIGINT Fundamentals capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise** and [255, 2026]; [258, 2026].

13.3.9.2 SIGINT Fundamentals instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise** and [255, 2026]; [258, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

13.3.9.3 SIGINT Fundamentals assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
SIGINT legal-authority and communications-security governance exercise	Completed **requirements matrix with source descriptors, caveats, and collection limits** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise	Completed **requirements matrix with source descriptors, caveats, and collection limits** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Spartans in Darkness: SIGINT legal-authority and communications-security governance exercise	Completed **requirements matrix with source descriptors, caveats, and collection limits** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

13.3.10 SIGINT Fundamentals refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [255, 2026]; [258, 2026] and **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**.

13.3.10.1 SIGINT Fundamentals refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**. The local signals begin with [255, 2026]; [258, 2026].

13.3.10.2 SIGINT Fundamentals claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**, and the source spine for these checks begins with [255, 2026]; [258, 2026].

13.3.11 SIGINT Fundamentals reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [255, 2026]; [258, 2026].

Triangulation anchors. In module 7's review-checklist section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise**. [255, 2026]; [258, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.

- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

13.3.12 SIGINT Fundamentals learning-path links: module map, overview, and curriculum atlas

Read this module in sequence with the curriculum orientation, its parent unit, and the adjacent modules so the evidence behind **SIGINT legal-authority and communications-security governance exercise; WWII Axis SIGINT: SIGINT legal-authority and communications-security governance exercise** carries forward intact. Source anchors for this module begin at [255, 2026]; [258, 2026].

Section 2, Section 12, Section 14

14 Modern SIGINT and Cryptography

14.0.1 Modern SIGINT and Cryptography figures and course links: visual evidence, source flow, and navigation

The module uses Figure 44 and Figure 41 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 12, Section 13, Section 15.
This module teaches the **Collection Management and Multi-INT Requirements Discipline** lane through a bounded, source-backed coursebook chapter. [258, 2026]; [260, 2026].

14.1 Collection Management and Multi-INT Requirements Discipline frame for Modern SIGINT and Cryptography: source context, topic focus, and reader task

Evidence anchor. Section 14; [258, 2026].

14.1.1 Modern SIGINT and Cryptography orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 14; [258, 2026].

14.1.2 Modern SIGINT and Cryptography conceptual primer: source context, core model, and reader task

This chapter teaches collection management as requirements discipline: a source method is considered only after the priority, authority, minimization rule, source risk, and evaluation plan are explicit. The chapter uses **Requirements-to-Evidence Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**.
The central distinction is to separate collection discipline concepts from operational recruitment, interception, or tasking procedures. Core topics include **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority; The Cryptographic Arms Race: E2E Encryption and Lawful Access**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [258, 2026]; [260, 2026].
Learners move from vocabulary and the **Requirements-to-Evidence Lens** distinction through topic lessons on **UKUSA and Five Eyes SIGINT Sharing** with evidence and misconception checks, then assemble a **requirements matrix with source descriptors, caveats, and collection limits** with safety and rights gates.

14.1.3 Modern SIGINT and Cryptography learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 14; [258, 2026].

- Connect **UKUSA and Five Eyes SIGINT Sharing and SIGINT metadata minimization and authority** to **Collection Management and Multi-INT Requirements Discipline** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **requirements matrix with source descriptors, caveats, and collection limits** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate collection discipline concepts from operational recruitment, interception, or tasking procedures; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as opportunistic collection, priority drift, over-collection, weak minimization, source exposure, and confusing availability with authority, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: collection material remains doctrinal and governance-oriented; it does not teach recruitment, interception, surveillance, or tasking procedures.

14.1.4 Modern SIGINT and Cryptography core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 14; [258, 2026].

Term	Working definition
Priority	the relative importance of an intelligence question
Source discipline	a broad evidence channel such as HUMINT, SIGINT, GEOINT, OSINT, or FININT
Minimization	the rule that limits acquisition, retention, or use of unnecessary information
Source protection	the duty to reduce risk to people, methods, and sensitive relationships
Evaluation	the feedback step that tests whether the evidence satisfied the requirement
Gray-zone indicator	an observable signal of ambiguous coercion below armed conflict thresholds
Proxy pattern	a relationship suggesting indirect sponsorship without confirmed operational control
UKUSA and Five Eyes SIGINT Sharing	Key terms: UKUSA, Five, Eyes.
SIGINT metadata minimization and authority	Key terms: SIGINT, metadata, minimization.

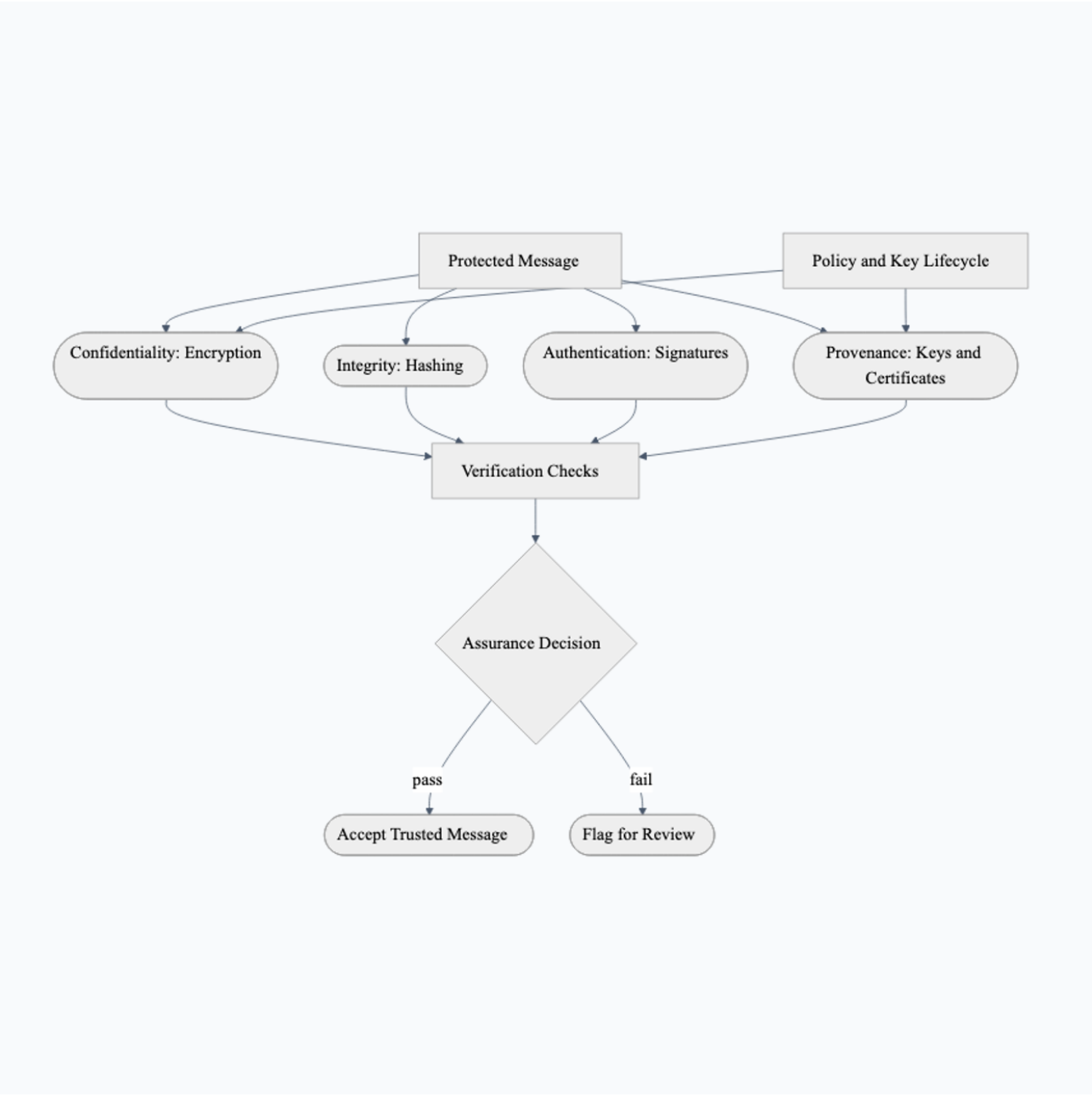


Figure 44: This diagram teaches the layered properties that together provide cryptographic assurance: confidentiality, integrity, authentication, and verifiable provenance. Its reader value is to make Protected Message, Verification Checks, and Policy and Key Lifecycle visible at a glance, with the signals intelligence sigint / modern sigint and cryptography section as the source section and defensive review as the boundary.

14.2 Requirements-to-Evidence Lens path for Modern SIGINT and Cryptography: lesson cluster, safe artifact, and review

Evidence anchor. Section 14; [258, 2026].

14.2.1 Modern SIGINT and Cryptography practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 14; [258, 2026].

14.2.2 Modern SIGINT and Cryptography topic lessons: source-backed concepts and transfer tasks

This module builds collection management as requirements discipline: a source method is considered only after the priority, authority, minimization rule, source risk, and evaluation plan are explicit. The sequence opens with **UKUSA and Five Eyes SIGINT Sharing**, **SIGINT metadata minimization and authority**, **The Cryptographic Arms Race: E2E Encryption and Lawful Access** and applies the **Requirements-to-Evidence Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 41; module overview Section 14; curriculum atlas Section 2.

Triangulation anchors. In module 8's topic-lessons section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

14.2.2.1 Lesson 1: UKUSA and Five Eyes SIGINT Sharing

Concept. UKUSA and Five Eyes SIGINT Sharing frames SIGINT as authority-bound collection with minimization, handling rules, and communications-security implications.

Why it matters. UKUSA and Five Eyes SIGINT Sharing matters in the **Collection Management and Multi-INT Requirements Discipline** lane because requirements decomposition and source-discipline fit evidence must stay separate from judgment; opportunistic collection is a common failure.

Source support. UKUSA and Five Eyes SIGINT Sharing rests on [041, 2026] and [042, 2026]. The most specific cited work observes: The materials, spanning 1945 to 2016, trace the development and functioning of the UKUSA Agreement underpinning intelligence cooperation among the US, UK, Canada, Australia, and New Zealand. Use them for the working definition that **UKUSA and Five Eyes SIGINT Sharing** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. Ground **UKUSA and Five Eyes SIGINT Sharing** in the evidence the row cites. [041, 2026] A collection page from Unredacted, a UK-based organization focused on declassified government records. It assembles over 70 documents obtained through a 2017 Freedom of Information Act legal challenge led by Privacy International, drawn from US agencies including the NSA, State Department, and Department of Defense. [042, 2026] A briefing from Unredacted examining previously classified Five Eyes documents released to Privacy International following a 2017 US freedom of information request. The materials, spanning 1945 to 2016, trace the development and functioning of the UKUSA Agreement underpinning intelligence cooperation among the US, UK, Canada, Australia, and New Zealand. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **UKUSA and Five Eyes SIGINT Sharing**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must name the source descriptor, the bounded claim about **UKUSA and Five Eyes SIGINT**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape this subject work as a **signal-evidence minimization card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that UKUSA and Five Eyes SIGINT Sharing replaces human review whenever evidence looks plausible.

Transfer task. Transfer **UKUSA and Five Eyes SIGINT Sharing** to a second module by preserving requirements decomposition and source-discipline fit, changing the source evidence, and naming a new reviewer.

14.2.2.2 Lesson 2: SIGINT metadata minimization and authority

Concept. SIGINT metadata minimization and authority frames SIGINT as authority-bound collection with minimization, handling rules, and communications-security implications.

Why it matters. SIGINT metadata minimization connects classroom vocabulary to Collection Management and Multi-INT Requirements Discipline practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. SIGINT metadata minimization and authority rests on [298, 2026] and [297, 2026]. The lead source's own note reads: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for the claim that **SIGINT metadata minimization and authority** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. For **SIGINT metadata minimization**, reason from the sources cited in this row. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. Build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must state the authority descriptor, the bounded claim about **SIGINT metadata minimization**, the minimization caveat, the uncertainty note, the collection boundary, and the reviewer accountable for the authorization. Shape this subject work as a **signal-evidence minimization card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that a named collection authority removes the minimization and retention limits on what may be kept.

Transfer task. Transfer **SIGINT metadata minimization** from this module to a second motif by preserving requirements decomposition and source-discipline fit, replacing action with audit, and naming the blocked use.

14.2.2.3 Lesson 3: The Cryptographic Arms Race: E2E Encryption and Lawful Access

Concept. The Cryptographic Arms Race: E2E Encryption and Lawful Access frames encryption as a policy and assurance trade-off among confidentiality, lawful process, communications security, and trust.

Why it matters. The Cryptographic Arms Race matters in the **Collection Management and Multi-INT Requirements Discipline** lane because requirements decomposition and source-discipline fit evidence must stay separate from judgment; opportunistic collection is a common failure.

Source support. The Cryptographic Arms Race: E2E Encryption and Lawful Access rests on [297, 2026] and [298, 2026]. The most specific cited work observes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for the claim that **The Cryptographic Arms Race: E2E**

Encryption and Lawful Access lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. Read **The Cryptographic Arms Race** against the works cited for this row. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **The Cryptographic Arms Race**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must name the source descriptor, the bounded claim about **Cryptographic Arms Race**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **The Cryptographic Arms Race** work as a **signal-evidence minimization card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that The Cryptographic Arms Race: E2E Encryption and Lawful Access is optional whenever separate collection discipline concepts from operational recruitment, interception, or tasking procedures feels inconvenient.

Transfer task. Transfer **The Cryptographic Arms Race** to a second module by preserving requirements decomposition and source-discipline fit, changing the source evidence, and naming a new reviewer.

14.2.2.4 Lesson 4: Communications-security history and lawful-access boundary

Concept. Communications-security history and lawful-access boundary connects the technical term to authority, minimization, communications-security risk, and public doctrine rather than interception mechanics.

Why it matters. Analysts use **Communications-security history** to separate collection discipline concepts from operational recruitment, interception, or tasking procedures. A defensible treatment names the judgment it enables for requirements decomposition and source-discipline fit review, the proof limit that opportunistic collection would otherwise hide, and the reviewer accountable for challenge.

Source support. Communications-security history and lawful-access boundary rests on [027, 2026] and [028, 2026]. Its anchor reference records: Learn a technique for communicating with your family in an emergency using a method used by spies. Use them for pinning down the scope of **Communications-security history and lawful-access boundary**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. For **Communications-security history**, work from the cited evidence behind this row. [027, 2026] Learn a technique for communicating with your family in an emergency using a method used by spies. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. Build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must state the authority descriptor, the bounded claim about **Communications-security history**, the minimization caveat, the uncertainty note, the collection boundary, and the reviewer accountable for the authorization. Shape this subject work as a **signal-evidence minimization card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Communications-security history**: that a named collection authority removes the minimization and retention limits on what may be kept.

Transfer task. Reuse the **Communications-security history** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

14.2.2.5 Lesson 5: RF-spectrum governance and communications-security

Concept. RF-spectrum governance and communications-security connects the technical term to authority, minimization, communications-security risk, and public doctrine rather than interception mechanics.

Why it matters. RF-spectrum governance connects classroom vocabulary to Collection Management and Multi-INT Requirements Discipline practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. RF-spectrum governance and communications-security rests on [043, 2026] and [044, 2026]. The most specific cited work observes: An informational guide from Bastille Networks explaining Technical Surveillance Countermeasures (TSCM), defined as security measures aimed at detecting and neutralizing surveillance devices to protect sensitive communications. Use them for pinning down the scope of **RF-spectrum governance and communications-security**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. For **RF-spectrum governance**, reason from the sources cited in this row. [043, 2026] An informational guide from Bastille Networks explaining Technical Surveillance Countermeasures (TSCM), defined as security measures aimed at detecting and neutralizing surveillance devices to protect sensitive communications. It traces TSCM origins to World War II and Cold War intelligence work and catalogues threat types such as radio-frequency transmitters, hidden cameras, and acoustic eavesdropping. [044, 2026] A reference page from the Granite Island Group describing a ten-level taxonomy of technical surveillance threats and the corresponding technical surveillance countermeasures (TSCM) inspections used to detect them. It explains that detection difficulty increases by roughly an order of magnitude at each level, grouping threats into clusters and beginning with low-power consumer-grade devices. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. Build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must state the authority descriptor, the bounded claim about **RF-spectrum governance**, the minimization caveat, the uncertainty note, the collection boundary, and the reviewer accountable for the authorization. Shape this subject work as a **signal-evidence minimization card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **RF-spectrum governance**: that a named collection authority removes the minimization and retention limits on what may be kept.

Transfer task. Reuse the **RF-spectrum governance** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

14.2.2.6 Lesson 6: SIGINT legal-authority and communications-security governance exercise

Concept. SIGINT legal-authority and communications-security governance exercise frames SIGINT as authority-bound collection with minimization, handling rules, and communications-security implications.

Why it matters. SIGINT legal-authority matters in the **Collection Management and Multi-INT Requirements Discipline** lane because requirements decomposition and source-discipline fit evidence must stay separate from judgment; opportunistic collection is a common failure.

Source support. SIGINT legal-authority and communications-security governance exercise rests on [045, 2026] and [046, 2026]. The lead source's own note reads: A web page from Murray Associates, a counterespionage consulting firm, explaining the technical surveillance countermeasures (TSCM) inspection process used to detect eavesdropping and surveillance devices in buildings. Use them for pinning down the scope of **SIGINT legal-authority and communications-security governance exercise**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. Ground **SIGINT legal-authority** in the evidence the row cites. [045, 2026] A service page from Pinkerton describing technical surveillance countermeasures used to detect and prevent corporate eavesdropping and protect intellectual property. It outlines examination

methods including infrared spectrum analysis to find heat signatures of hidden devices, radio frequency analysis to identify wireless audio bugs, and physical inspection for tampered equipment or poor security practices. [046, 2026] A web page from Murray Associates, a counterespionage consulting firm, explaining the technical surveillance countermeasures (TSCM) inspection process used to detect eavesdropping and surveillance devices in buildings. It outlines a three-phase methodology: a pre-inspection planning discussion, an on-site evaluation combining visual examination, technical instrumentation, and information-security review, and a post-inspection written report with findings and recommendations. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **SIGINT legal-authority**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must state the authority descriptor, the bounded claim about **SIGINT legal-authority and communications-security governance**, the minimization caveat, the uncertainty note, the collection boundary, and the reviewer accountable for the authorization. Shape **SIGINT legal-authority** work as a **signal-evidence minimization card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **SIGINT legal-authority**: that a named collection authority removes the minimization and retention limits on what may be kept.

Transfer task. Transfer **SIGINT legal-authority** from this module to a second motif by preserving requirements decomposition and source-discipline fit, replacing action with audit, and naming the blocked use.

14.2.2.7 Lesson 7: Linear Junction Detectors RF Spectrum: RF-spectrum governance and communications-security

Concept. Linear Junction Detectors RF Spectrum: RF-spectrum governance and communications-security connects the technical term to authority, minimization, communications-security risk, and public doctrine rather than interception mechanics.

Why it matters. Analysts use **Linear Junction Detectors RF Spectrum** to separate collection discipline concepts from operational recruitment, interception, or tasking procedures. A defensible treatment names the judgment it enables for requirements decomposition and source-discipline fit review, the proof limit that opportunistic collection would otherwise hide, and the reviewer accountable for challenge.

Source support. Linear Junction Detectors RF Spectrum: RF-spectrum governance and communications-security rests on [309, 2026], [310, 2026], and [300, 2026]. Its anchor reference records: The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. Use them for fixing what **Linear Junction Detectors RF Spectrum: RF-spectrum governance and communications-security** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. Read **Linear Junction Detectors RF Spectrum** against the works cited for this row. [309, 2026] An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection. [310, 2026] The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Linear Junction Detectors RF Spectrum**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must state the authority descriptor, the bounded claim about **Linear Junction Detectors RF Spectrum**, the minimization caveat, the uncertainty note, the collection boundary, and the reviewer accountable for the authorization. Shape **Linear Junction Detectors RF Spectrum** work as a **signal-evidence minimization card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Linear Junction Detectors RF Spectrum**: that a named collection authority removes the minimization and retention limits on what may be kept.

Transfer task. Apply this module's safe boundary for **Linear Junction Detectors RF Spectrum** to another artifact while keeping requirements decomposition and source-discipline fit and reviewer ownership explicit.

14.2.2.8 Lesson 8: Steganography detection-literacy and communications-security

Concept. Steganography detection-literacy and communications-security connects the technical term to authority, minimization, communications-security risk, and public doctrine rather than interception mechanics.

Why it matters. Analysts use **Steganography detection-literacy** to separate collection discipline concepts from operational recruitment, interception, or tasking procedures. A defensible treatment names the judgment it enables for requirements decomposition and source-discipline fit review, the proof limit that opportunistic collection would otherwise hide, and the reviewer accountable for challenge.

Source support. Steganography detection-literacy and communications-security rests on [028, 2026]. Use it for the working definition that **Steganography detection-literacy and communications-security** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. Ground **Steganography detection-literacy** in the evidence the row cites. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. Build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must state the authority descriptor, the bounded claim about **Steganography detection-literacy**, the minimization caveat, the uncertainty note, the collection boundary, and the reviewer accountable for the authorization. Shape this subject work as a **signal-evidence minimization card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Steganography detection-literacy**: that a named collection authority removes the minimization and retention limits on what may be kept.

Transfer task. Transfer **Steganography detection-literacy** from this module to a second motif by preserving requirements decomposition and source-discipline fit, replacing action with audit, and naming the blocked use.

14.2.2.9 Lesson 9: Signal Authentication in the Deepfake Era

Concept. Signal Authentication in the Deepfake Era applies Signal, Authentication, in within Collection Management and Multi-INT Requirements Discipline: learners use separate collection discipline concepts from operational recruitment, interception, or tasking procedures and requirements decomposition and source-discipline fit evidence before any judgment moves forward.

Why it matters. Without explicit treatment of **Signal Authentication**, opportunistic collection undermines requirements decomposition and source-discipline fit review; the lesson builds the habit to separate collection discipline concepts from operational recruitment, interception, or tasking procedures.

Source support. Signal Authentication in the Deepfake Era rests on [018, 2026]. Its anchor reference records: It argues that as AI makes deepfakes and synthetic communications easier, trust in digital channels erodes, paradoxically increasing the value of traditional human intelligence methods. Use it for fixing what **Signal Authentication in the Deepfake Era** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. Ground **Signal Authentication** in the evidence the row cites. [018, 2026] A Nextgov article reporting on an essay in the CIA's Studies in Intelligence journal by RAND researcher Thomas Mulligan. It argues that as AI makes deepfakes and synthetic communications easier, trust in digital channels erodes, paradoxically increasing the value of traditional human intelligence methods. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Signal Authentication**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this requirements decomposition and source-discipline fit topic. The artifact must name the source descriptor, the bounded claim about **Signal Authentication in the Deepfake**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Signal Authentication** work as a **signal-evidence minimization card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that Signal Authentication in the Deepfake Era replaces human review whenever evidence looks plausible.

Transfer task. Transfer **Signal Authentication** to a second module by preserving requirements decomposition and source-discipline fit, changing the source evidence, and naming a new reviewer.

14.2.3 Modern SIGINT and Cryptography worked safe example: synthetic inputs, evidence, and review

Worked example: a synthetic policy cell compares public indicators of hybrid pressure against an approved collection plan for a benign border-disruption exercise. [258, 2026]; [260, 2026].

Triangulation anchors. In module 8's worked-example section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **signals-intelligence governance**. Learners use a **signal-evidence minimization card** and keep this boundary visible: No interception, decryption, surveillance target selection, or collection-expansion guidance.

Frame. The classroom question centers on **UKUSA and Five Eyes SIGINT Sharing**. Excluded actions stay explicit, and the **Requirements-to-Evidence Lens** planning question is: What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit?

Inputs. For the **UKUSA and Five Eyes SIGINT Sharing** scenario, use public notices, synthetic interview summaries, public logistics records, and an instructor scope card. The Requirements-to-Evidence Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **UKUSA and Five Eyes SIGINT Sharing**, students rank requirements, choose the least intrusive source discipline, list excluded actions, and evaluate evidence quality. Pause whenever an inference about UKUSA and Five Eyes SIGINT Sharing appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **UKUSA and Five Eyes SIGINT Sharing** classroom scenario; unit artifact = signal-evidence minimization card; evidence = allowed inputs; method = requirements decomposition and source-discipline fit; output = a requirements-to-evidence matrix with discipline fit, source caveats, minimization notes, and gaps; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **UKUSA and Five Eyes SIGINT Sharing** as "Requirements-to-Evidence Lens confirms it" is not enough. The revision ties the claim to requirements decomposition and source-discipline fit, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **UKUSA and Five Eyes SIGINT Sharing** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

14.2.4 Modern SIGINT and Cryptography practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Requirements-to-Evidence Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**.

Triangulation anchors. In module 8's practice-sequence section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare UKUSA and Five Eyes SIGINT Sharing, SIGINT metadata minimization and authority, The Cryptographic Arms Race: E2E Encryption and Lawful Access; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Collection Management and Multi-INT Requirements Discipline** lane.
2. Frame	Answer the lens question: What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for UKUSA and Five Eyes SIGINT Sharing: requirements matrix with source descriptors, caveats, and collection limits.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the signal-evidence minimization card fields for UKUSA and Five Eyes SIGINT Sharing.	Unit profile note.	Evidence artifacts include authority boundary note, minimization field.
4. Challenge	Test the misconception that UKUSA and Five Eyes SIGINT Sharing replaces human review whenever evidence looks plausible.	Failure-mode note.	The artifact applies the key distinction: separate collection discipline concepts from operational recruitment, interception, or tasking procedures.

Move	Learner action	Output	Check
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

14.2.4.1 Modern SIGINT and Cryptography instructor notes: source reasoning, review points, and studio focus Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**. [258, 2026]; [260, 2026].

14.2.4.2 Modern SIGINT and Cryptography extension exercise: peer validation and refresh trigger review Evidence anchor. Section 14; [258, 2026].

Have learners swap artifacts and apply the **Requirements-to-Evidence Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**.

14.2.5 Modern SIGINT and Cryptography knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 14; [258, 2026].

1. Explain how **UKUSA and Five Eyes SIGINT Sharing** is defined here; name the source descriptor that supports the definition.
2. Contrast **UKUSA and Five Eyes SIGINT Sharing** with **SIGINT metadata minimization and authority** using the **Requirements-to-Evidence Lens** artifact fields.
3. Identify one failure mode from the **Collection Management and Multi-INT Requirements Discipline** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which gray-zone indicator changes the least-intrusive source choice without crossing into operational tasking?
5. Correct this misconception: that UKUSA and Five Eyes SIGINT Sharing replaces human review whenever evidence looks plausible.

14.2.5.1 Modern SIGINT and Cryptography answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **UKUSA and Five Eyes SIGINT Sharing** without source evidence, uncertainty, or a safe transfer task.

14.3 Modern SIGINT and Cryptography assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 14; [258, 2026].

14.3.1 Modern SIGINT and Cryptography evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 14; [258, 2026].

14.3.2 Modern SIGINT and Cryptography transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 14; [258, 2026].

14.3.2.1 Modern SIGINT and Cryptography lineage and source tradition: profile, concepts, and first anchors This sits in the **Collection Management and Multi-INT Requirements Discipline** lineage: requirements-driven, authority-bounded collection where priorities, legal basis, minimization, source protection, and evaluation are explicit. [258, 2026]; [260, 2026].

14.3.2.2 Modern SIGINT and Cryptography working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 14; [258, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**, with provenance and reviewability throughout.

14.3.2.3 Modern SIGINT and Cryptography knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** accountable requirements, source-discipline choices, minimization rules, source-risk notes, and evaluation criteria. [258, 2026]; [260, 2026].
- **Transforms:** priority mapping, source-discipline fit, least-intrusive evidence selection, and feedback review.
- **Outputs:** requirements matrix, collection-limit note, source-quality card, and gap list.
- **Failure modes:** recruitment or interception drift, over-collection, weak minimization, and source exposure.

14.3.2.4 Modern SIGINT and Cryptography transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 14; [258, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**.
- **Evidence contract:** keep the **Collection Management and Multi-INT Requirements Discipline** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as requirements matrix, collection-limit note, source-quality card, and gap list that another reviewer can audit.

14.3.2.5 Modern SIGINT and Cryptography profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 14; [258, 2026].

The matched profile emphasizes requirements-driven, authority-bounded collection where priorities, legal basis, minimization, source protection, and evaluation are explicit. The method stack is priority mapping, requirement decomposition, source-discipline fit, coverage-gap review, legal-authority check, and collection-feedback loop; the local topic cluster is **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**.

14.3.3 Modern SIGINT and Cryptography evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 14; [258, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Collection Management and Multi-INT Requirements Discipline** profile tells reviewers what evidence is strong enough for the module artifact built around **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**.

14.3.3.1 Modern SIGINT and Cryptography guide source spine: inherited keys and local citation roles Primary guide citations: [258, 2026]; [260, 2026]; [261, 2026]; [275, 2026]; [276, 2026]; [283, 2026]; [286, 2026]; [293, 2026]; [295, 2026]; [041, 2026]; [042, 2026]; [027, 2026]; [028, 2026]; [043, 2026]; [044, 2026]; [045, 2026]; [046, 2026]; [018, 2026]; [298, 2026]; [297, 2026]; [309, 2026]; [310, 2026]; [300, 2026].

14.3.3.2 Modern SIGINT and Cryptography verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [258, 2026]; [260, 2026].

Tier	What counts	How it is used
Source guide	[258, 2026]; [260, 2026]; [261, 2026]; [275, 2026]; [276, 2026]; [283, 2026]; [286, 2026]; [293, 2026]; [295, 2026]; [041, 2026]; [042, 2026]; [027, 2026]; [028, 2026]; [043, 2026]; [044, 2026]; [045, 2026]; [046, 2026]; [018, 2026]; [298, 2026]; [297, 2026]; [309, 2026]; [310, 2026]; [300, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 8's source-canon section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority** and [258, 2026]; [260, 2026], but only directly verified source URLs are encoded as citations.

14.3.3.3 Modern SIGINT and Cryptography intelligence practice lens: evidence artifact and safety check Practice lens: **Requirements-to-Evidence Lens** for **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**. [258, 2026]; [260, 2026].

Planning question: What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit?

Evidence artifact: requirements matrix with source descriptors, caveats, and collection limits.

Validation rule: show priority, authority, minimization, corroboration, and source quality before any claim is reused. Applied to **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**.

Handoff contract: deliver metadata-rich evidence packets, not unscoped data piles or implicit targeting requests.

Safety check: exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure.

14.3.3.4 Modern SIGINT and Cryptography runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 14; [258, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	8.99	8.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Modern SIGINT and Cryptography to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Bounded autonomy, procurement, incident-response, and assurance studio	8.101	8.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Modern SIGINT and Cryptography	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Model-card, recoverability, retention, and learner-support evidence package	8.102	8.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Modern SIGINT and Cryptography	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
UKUSA and Five Eyes SIGINT Sharing	8.1	8.1 UKUSA and Five Eyes SIGINT Sharing	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
SIGINT metadata minimization and authority	8.2	8.2 source title transformed into safe curriculum treatment; original: Bulk Collection, Metadata Analysis, and Legal Frameworks	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
The Cryptographic Arms Race: E2E Encryption and Lawful Access	8.3	8.3 The Cryptographic Arms Race: E2E Encryption and Lawful Access	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Communications-security history and lawful-access boundary	8.4	8.4 source title transformed into safe curriculum treatment; original: Covert Communications Tradecraft: OTPs, Burst Transmission, Digital Dead Drops	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
RF-spectrum governance and communications-security	8.5	8.5 source title transformed into safe curriculum treatment; original: Radio Frequency Intelligence (RFINT) and Technical Surveillance	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
SIGINT legal-authority and communications-security governance exercise	8.6	8.6 source title transformed into safe curriculum treatment; original: Technical Surveillance Countermeasures (TSCM): Threat Levels and Detection	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
RF-spectrum governance and communications-security	8.7	8.7 source title transformed into safe curriculum treatment; original: Non-Linear Junction Detectors, RF Spectrum Analysis, Infrared Imaging	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Steganography detection-literacy and communications-security	8.8	8.8 source title transformed into safe curriculum treatment; original: Steganography: LSB, DCT, and Network-Layer Methods	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Signal Authentication in the Deepfake Era	8.9	8.9 Signal Authentication in the Deepfake Era	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

14.3.3.5 Modern SIGINT and Cryptography reusable subsection contract: topic rows, artifacts, and safety duties Evidence anchor. Section 14; [258, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
UKUSA and Five Eyes SIGINT Sharing	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
SIGINT metadata minimization and authority	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
The Cryptographic Arms Race: E2E Encryption and Lawful Access	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Communications-security history and lawful-access boundary	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

Lesson topic	Practice lens	Evidence artifact	Safety check
RF-spectrum governance and communications-security	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
SIGINT legal-authority and communications-security governance exercise	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
Linear Junction Detectors RF Spectrum: RF-spectrum governance and communications-security	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Steganography detection-literacy and communications-security	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Signal Authentication in the Deepfake Era	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

14.3.3.6 Modern SIGINT and Cryptography annotated source ledger: real titles and local contribution Each source cited by this **Collection Management and Multi-INT Requirements Discipline** module is paired below with its real title and a one-line note on what it contributes to **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**.

Source	Cited work	What it contributes	Status
[258, 2026]	OpenAPI Specification	The official OpenAPI Initiative publications page, serving as a central index for the OpenAPI Specification and related standards including the Arazzo and Overlay specifications. It provides access to multiple specification versions (2.0, 3.0, 3.1, and 3.2) and their corresponding downloadable schemas identified by release date, along with a registry of extensions, formats, media types, and other resources.	verified source-guide
[260, 2026]	Decentralized Identifiers (DIDs) v1.0	The W3C Recommendation for Decentralized Identifiers (DIDs) v1.0, published July 2022, defining a type of identifier that enables verifiable digital identity without reliance on a centralized registration authority. It specifies DID syntax (a scheme, method name, and method-specific identifier) and the DID document data model, which expresses verification methods, services, controllers, and verification relationships for authentication and assertion.	verified source-guide
[261, 2026]	RFC 9110: HTTP Semantics	RFC 9110, the official IETF standards document defining the core semantics and architecture of HTTP, published in June 2022 and consolidating nine earlier RFCs. It establishes terminology and protocol aspects shared across HTTP versions, including methods, status codes, header fields, content negotiation, conditional and range requests, authentication, and the http and https URI schemes.	verified source-guide
[275, 2026]	Fact Sheet: New Rule on the Accessibility of Web Content and Mobile Apps Provided by State and Local Governments	A US Department of Justice fact sheet explaining the 2024 ADA Title II rule requiring state and local governments to make their web content and mobile apps accessible. It establishes WCAG 2.1 Level AA as the technical standard, applies to entities such as schools, courts, libraries, and transit agencies, and sets compliance deadlines of April 2027 for larger jurisdictions and April 2028 for smaller ones.	verified source-guide

Source	Cited work	What it contributes	Status
[276, 2026]	What is a Data Protection Impact Assessment and When Is This Mandatory?	A European Data Protection Board FAQ page, part of its data protection guide for small businesses, explaining Data Protection Impact Assessments (DPIAs) and when they are mandatory. It describes a DPIA as a written assessment of the impact of a planned processing operation, required when processing poses high risks to individuals' rights.	verified source-guide
[283, 2026]	Recommendation of the Council on Open Government	An OECD legal instrument document reproducing the Recommendation of the Council on Open Government (OECD/LEGAL/0438), adopted on 14 December 2017. It defines open government as a culture of governance promoting transparency, integrity, accountability, and stakeholder participation in support of democracy and inclusive growth.	verified source-guide
[286, 2026]	Model Cards for Model Reporting	The arXiv abstract for "Model Cards for Model Reporting" (2018) by Mitchell, Wu, Zaldivar, and colleagues, which introduces a framework for transparent documentation of machine learning models. Model cards are short accompanying documents that report a model's benchmarked performance across varied conditions, including different cultural, demographic, and phenotypic groups, along with intended use, evaluation methodology, and deployment considerations.	verified source-guide
[293, 2026]	Inventory of NARA Artificial Intelligence (AI) Use Cases	The National Archives and Records Administration (NARA) official inventory of its artificial intelligence use cases, documenting 14 projects across deployed, pilot, and planned stages. Deployed efforts include workplace productivity tools, automated tagging for museum experiences, and historical record retrieval, while pilots cover PII detection and redaction, semantic search, and metadata generation, and planned work targets FOIA processing and public search.	verified source-guide
[295, 2026]	M-25-22: Driving Efficient Acquisition of Artificial Intelligence in Government	OMB Memorandum M-25-22 (April 3, 2025), Driving Efficient Acquisition of Artificial Intelligence in Government, issued under Executive Order 13960 and related directives. It provides guidance to federal agencies for acquiring effective and trustworthy AI in a timely, cost-effective manner, and rescinds and replaces earlier memorandum M-24-18.	verified source-guide
[041, 2026]	Five Eyes FOIA disclosures	A collection page from Unredacted, a UK-based organization focused on declassified government records. It assembles over 70 documents obtained through a 2017 Freedom of Information Act legal challenge led by Privacy International, drawn from US agencies including the NSA, State Department, and Department of Defense.	verified source-guide

Source	Cited work	What it contributes	Status
[042, 2026]	Five Eyes FOIA disclosures: key documents	A briefing from Unredacted examining previously classified Five Eyes documents released to Privacy International following a 2017 US freedom of information request. The materials, spanning 1945 to 2016, trace the development and functioning of the UKUSA Agreement underpinning intelligence cooperation among the US, UK, Canada, Australia, and New Zealand.	verified source-guide
[027, 2026]	The Dead Drop: Design a Communications Method Like a Spy	Learn a technique for communicating with your family in an emergency using a method used by spies.	original source-guide
[028, 2026]	Cited source (see bibliography)	See bibliography for scope.	original source-guide
[043, 2026]	Technical Surveillance Countermeasures (TSCM) - Bastille Networks	An informational guide from Bastille Networks explaining Technical Surveillance Countermeasures (TSCM), defined as security measures aimed at detecting and neutralizing surveillance devices to protect sensitive communications. It traces TSCM origins to World War II and Cold War intelligence work and catalogues threat types such as radio-frequency transmitters, hidden cameras, and acoustic eavesdropping.	verified source-guide
[044, 2026]	Technical Surveillance Threat Levels - Granite Island Group	A reference page from the Granite Island Group describing a ten-level taxonomy of technical surveillance threats and the corresponding technical surveillance countermeasures (TSCM) inspections used to detect them. It explains that detection difficulty increases by roughly an order of magnitude at each level, grouping threats into clusters and beginning with low-power consumer-grade devices.	verified source-guide
[045, 2026]	TSCM / Technical Surveillance Countermeasures - Pinkerton	A service page from Pinkerton describing technical surveillance countermeasures used to detect and prevent corporate eavesdropping and protect intellectual property. It outlines examination methods including infrared spectrum analysis to find heat signatures of hidden devices, radio frequency analysis to identify wireless audio bugs, and physical inspection for tampered equipment or poor security practices.	verified source-guide
[046, 2026]	The TSCM Inspection Process / by Murray Associates TSCM	A web page from Murray Associates, a counterespionage consulting firm, explaining the technical surveillance countermeasures (TSCM) inspection process used to detect eavesdropping and surveillance devices in buildings. It outlines a three-phase methodology: a pre-inspection planning discussion, an on-site evaluation combining visual examination, technical instrumentation, and information-security review, and a post-inspection written report with findings and recommendations.	verified source-guide

Source	Cited work	What it contributes	Status
[018, 2026]	Old-school spycraft could make a comeback as AI undermines trust	A Nextgov article reporting on an essay in the CIA's Studies in Intelligence journal by RAND researcher Thomas Mulligan. It argues that as AI makes deepfakes and synthetic communications easier, trust in digital channels erodes, paradoxically increasing the value of traditional human intelligence methods.	verified source-guide
[298, 2026]	Intelligence Community Directives	Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations.	original source-guide
[297, 2026]	Intelligence Community Directive 203: Analytic Standards	Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products.	original source-guide
[309, 2026]	STIX Version 2.1	An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection.	verified source-guide
[310, 2026]	TAXII Version 2.1	The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe).	verified source-guide
[300, 2026]	MITRE ATLAS	MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy.	original source-guide

Where this sits. This module's overview is Section 14; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

14.3.4 Modern SIGINT and Cryptography governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 14; [258, 2026].

14.3.5 Modern SIGINT and Cryptography analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 8's governance-boundary section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **Collection Management and Multi-INT Requirements Discipline** for **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**. [258, 2026]; [260, 2026].

Curriculum topic spine: UKUSA and Five Eyes SIGINT Sharing, **SIGINT metadata minimization and authority**, **The Cryptographic Arms Race: E2E Encryption and Lawful Access**. **Verified anchor cluster:** [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]; [Archives and Administration, 1981]; [Agency, 2026g]; [of the Director of National Intelligence, 2026d].

Conceptual depth: requirements-driven, authority-bounded collection where priorities, legal basis, minimization, source protection, and evaluation are explicit.

Method stack: priority mapping, requirement decomposition, source-discipline fit, coverage-gap review, legal-authority check, and collection-feedback loop.

Composability contract: requirements, authorities, source disciplines, collection notes, retention limits, caveats, and evaluation metrics remain separable.

Known failure modes: opportunistic collection, priority drift, over-collection, weak minimization, source exposure, and confusing availability with authority.

Defensive boundary: collection material remains doctrinal and governance-oriented; it does not teach recruitment, interception, surveillance, or tasking procedures. Applied to **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**.

Anchor	Why it matters here
[Community, 2026]	Official public explanation of the intelligence cycle, collection disciplines, dissemination, evaluation, oversight, and partners. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026c]	Official prioritization directive for translating national intelligence priorities into collection, analysis, risk management, and responsiveness evaluation. Checked as of 2026-05-21; role: curriculum_anchor.
[of Staff, 2026]	Official joint-doctrine landing page for the keystone publication on joint intelligence principles, products, services, and assessments. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence and Agency, 2024]	Official IC OSINT strategy for professionalizing OSINT, integrated collection management, open-source sharing, innovation, and tradecraft. Checked as of 2026-05-21; role: curriculum_anchor.
[Archives and Administration, 1981]	Official legal anchor for intelligence authorities, rights-aware collection, analytic competition, oversight, and source-method protection. Checked as of 2026-05-21; role: curriculum_anchor.
[Agency, 2026g]	Official NSA public explanation of FISA oversight for signals intelligence collection governed by statutory and court-authorized controls. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026d]	Official sourcing directive for traceability, citations, source descriptors, and source summaries. Checked as of 2026-05-21; role: curriculum_anchor.

14.3.5.1 Modern SIGINT and Cryptography evidence standard and citation floor: source families and discovery limits Official guidance supplies governance, safety, and legal constraints for the **Collection Management and Multi-INT Requirements Discipline** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [258, 2026]; [260, 2026].

14.3.6 Modern SIGINT and Cryptography agentic boundary: assist, approve, block, and record

Evidence anchor. Section 14; [258, 2026].

AGEINT translation is bounded by the **Collection Management and Multi-INT Requirements Discipline** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**.

14.3.6.1 Modern SIGINT and Cryptography permitted defensive utility: curriculum uses and safe outputs Evidence anchor. Section 14; [258, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**.

14.3.6.2 Modern SIGINT and Cryptography excluded operational boundary: blocked actions and stop rules Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [258, 2026]; [260, 2026] and **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

14.3.7 Modern SIGINT and Cryptography governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 14; [258, 2026].

Governance is practiced as a gate on the **Collection Management and Multi-INT Requirements Discipline** lane. Learners use the **Requirements-to-Evidence Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain,

and when an agent-assisted artifact must stop for human review while using **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**.

14.3.7.1 Modern SIGINT and Cryptography governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [258, 2026]; [260, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Collection Management and Multi-INT Requirements Discipline** failure modes and the **Requirements-to-Evidence Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

14.3.7.2 Modern SIGINT and Cryptography evidence package handoff: appendices, records, and reuse

Evidence anchor. Section 14; [258, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Requirements-to-Evidence Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**.

14.3.7.3 Modern SIGINT and Cryptography current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**. [258, 2026]; [260, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_intelligence_gov_how_ic_works` for **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**?	How the IC Works; lane `governed_intelligence_cycle`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official public explanation of the intelligence cycle, collection disciplines, dissemination, evaluation, oversight, and partners.
What does the module inherit from `official_odni_icd_204` for **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**?	Intelligence Community Directive 204: National Intelligence Priorities Framework; lane `collection_management`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official prioritization directive for translating national intelligence priorities into collection, analysis, risk management, and responsiveness evaluation.
What does the module inherit from `official_joint_pub_2_0` for **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**?	JP 2-0: Joint Intelligence; lane `collection_management`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official joint-doctrine landing page for the keystone publication on joint intelligence principles, products, services, and assessments.
What does the module inherit from `official_ic_osint_strategy` for **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**?	The INT of First Resort: The IC OSINT Strategy 2024-2026; lane `osint_geoint`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official IC OSINT strategy for professionalizing OSINT, integrated collection management, open-source sharing, innovation, and tradecraft.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 14; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

14.3.8 Modern SIGINT and Cryptography assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 14; [258, 2026].

14.3.9 Modern SIGINT and Cryptography assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 14; [258, 2026].

14.3.9.1 Modern SIGINT and Cryptography capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority** and [258, 2026]; [260, 2026].

14.3.9.2 Modern SIGINT and Cryptography instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority** and [258, 2026]; [260, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

14.3.9.3 Modern SIGINT and Cryptography assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
UKUSA and Five Eyes SIGINT Sharing	Completed **requirements matrix with source descriptors, caveats, and collection limits** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
SIGINT metadata minimization and authority	Completed **requirements matrix with source descriptors, caveats, and collection limits** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
The Cryptographic Arms Race: E2E Encryption and Lawful Access	Completed **requirements matrix with source descriptors, caveats, and collection limits** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

14.3.10 Modern SIGINT and Cryptography refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [258, 2026]; [260, 2026] and **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**.

14.3.10.1 Modern SIGINT and Cryptography refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**. The local signals begin with [258, 2026]; [260, 2026].

14.3.10.2 Modern SIGINT and Cryptography claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**, and the source spine for these checks begins with [258, 2026]; [260, 2026].

14.3.11 Modern SIGINT and Cryptography reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [258, 2026]; [260, 2026].

Triangulation anchors. In module 8's review-checklist section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority**. [258, 2026]; [260, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

14.3.12 Modern SIGINT and Cryptography learning-path links: module map, overview, and curriculum atlas

Read this module in sequence with the curriculum orientation, its parent unit, and the adjacent modules so the evidence behind **UKUSA and Five Eyes SIGINT Sharing; SIGINT metadata minimization and authority** carries forward intact. Source anchors for this module begin at [258, 2026]; [260, 2026].

Section 2, Section 12, Section 13, Section 15

15 OPEN SOURCE INTELLIGENCE (OSINT)

15.1 OPEN SOURCE INTELLIGENCE (OSINT) learning spine and source route: unit purpose, module order, and evidence handoff

Evidence anchor. Section 15; [251, 2026].

15.1.1 open-source intelligence governance discipline spine: domain question and learning focus

Evidence anchor. Section 15; [251, 2026].
This unit teaches **open-source intelligence governance**. OSINT work turns public availability into evaluated intelligence only after provenance, terms, reliability, minimization, and reproducibility are reviewed.

15.1.2 open-source intelligence governance source-use contract: citation roles and evidence limits

Evidence anchor. Section 15; [251, 2026].
Use IC OSINT strategy and tool-governance anchors for public-source quality, transparency, and ethics claims.

15.1.3 open-source intelligence governance practice artifact: recurring packet and retained evidence

Evidence anchor. Section 15; [251, 2026].
The recurring practice artifact is a **OSINT provenance and minimization matrix** that draws on provenance chain, terms-of-use note, corroboration matrix, and minimization decision. The unit keeps its learning spine explicit. Learners document source origin, recency, independence, transformation history, and what cannot be inferred.

15.1.4 open-source intelligence governance safety boundary: accountable, synthetic, and evidence-bounded limits

No exposed-service lookup, credentialed access, identity exposure, doxxing, or live collection expansion.
This unit introduces the part's governing question, evidence artifacts, source-support spine, and capstone thread before the individual modules begin. [251, 2026]; [253, 2026].
Learners carry one unit capstone thread through the part: define an accountable intelligence question, bind it to source-quality constraints, produce a reviewable artifact, test the artifact against failure modes, and hand it off with enough context for another analyst or instructor to audit. The capstone remains public, synthetic, or owned-lab throughout; its first source anchors are [251, 2026]; [253, 2026].
This unit's deliverables are a source-canon card, claim/evidence ledger, safe-practice lab packet, failure-mode note, instructor rubric, and debrief memo. The full source-lane and evidence-package ledgers appear in the orientation and appendices; this unit introduction keeps only the learner-facing spine for [251, 2026]; [253, 2026].
This unit's safety gates are scope authorization, rights review, data provenance, tool allowlisting, human oversight, rollback, and evidence-bounded output. A missing gate turns the activity into a tabletop, audit, or written governance exercise until the gate is restored against [251, 2026]; [253, 2026].
Capstone thread:

Phase	Artifact	Review gate
Question	accountable learning question and excluded-action list	instructor confirms scope, allowed data, and rights impact
Source canon	source-lane map with guide citations, verified anchors, and refresh dates	citation keys resolve and source identity lock remains stable
Evidence ledger	claim, evidence, uncertainty, confidence, and reviewer register	every material claim has a source, caveat, and owner
Safe lab	synthetic or public dataset packet, tool allowlist, and stop conditions	no live target, private data, external action, or unsafe cyber-physical step
Assurance	evaluation rubric, failure-mode drill, rights map, and remediation note	human reviewer signs off before presentation or reuse
Debrief	capstone memo with lessons, residual risk, refresh triggers, and handoff owner	all unresolved questions and future approvals are explicit

Research lane: Open-Source and Geospatial Intelligence Integrity. Core anchors: [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]. Conceptual focus: public-source discovery converted into accountable intelligence through provenance, corroboration, minimization, and relevance tests. Composability contract: collection notes, source metadata, transformations, caveats, and analytic judgments remain separately exportable. **Practice lens:** Requirements-to-Evidence Lens; What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit? [251, 2026]; [253, 2026].

15.1.5 OPEN SOURCE INTELLIGENCE (OSINT) visual navigation and module map: evidence flow, order, and safety cues

The unit uses Figure 45 and Figure 46 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 14, Section 16.

15.1.6 OPEN SOURCE INTELLIGENCE (OSINT) module roster and source-lane inventory: citations, lanes, and learner route

Module	Section reference	Source spine
OSINT Foundations	Section 16	[251, 2026]; [253, 2026]; [269, 2026]; [273, 2026]; [274, 2026]; [275, 2026]; [286, 2026]; [287, 2026]; [292, 2026]; [047, 2026]; [048, 2026]; [049, 2026]; [301, 2026]; [298, 2026]; [297, 2026].
OSINT Techniques and Tools	Section 17	[251, 2026]; [252, 2026]; [269, 2026]; [276, 2026]; [277, 2026]; [284, 2026]; [288, 2026]; [289, 2026]; [293, 2026]; [050, 2026]; [051, 2026]; [052, 2026]; [053, 2026]; [054, 2026]; [055, 2026]; [056, 2026].

Module	Section reference	Source spine
GEOINT and Imagery Intelligence	Section 18	[253, 2026]; [255, 2026]; [270, 2026]; [278, 2026]; [279, 2026]; [283, 2026]; [290, 2026]; [291, 2026]; [294, 2026]; [057, 2026]; [058, 2026]; [059, 2026]; [060, 2026]; [301, 2026]; [298, 2026]; [302, 2026]; [297, 2026].

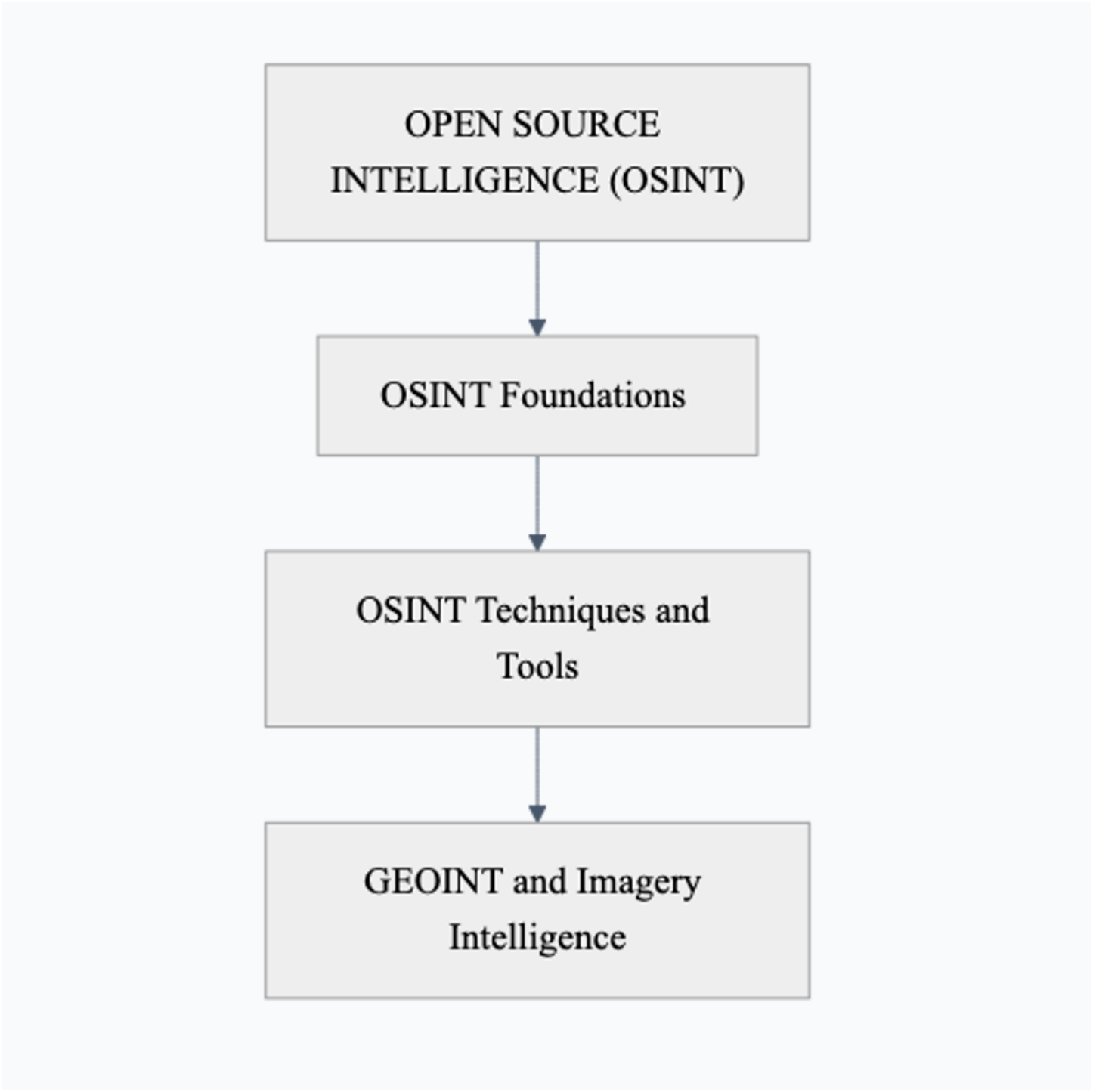


Figure 45: The unit module map traces the part's chapters as a linear reading sequence. It is anchored to the open source intelligence osint section; use it to inspect 3 module nodes in the unit's ordered, source-backed reading sequence from its first module to its last while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

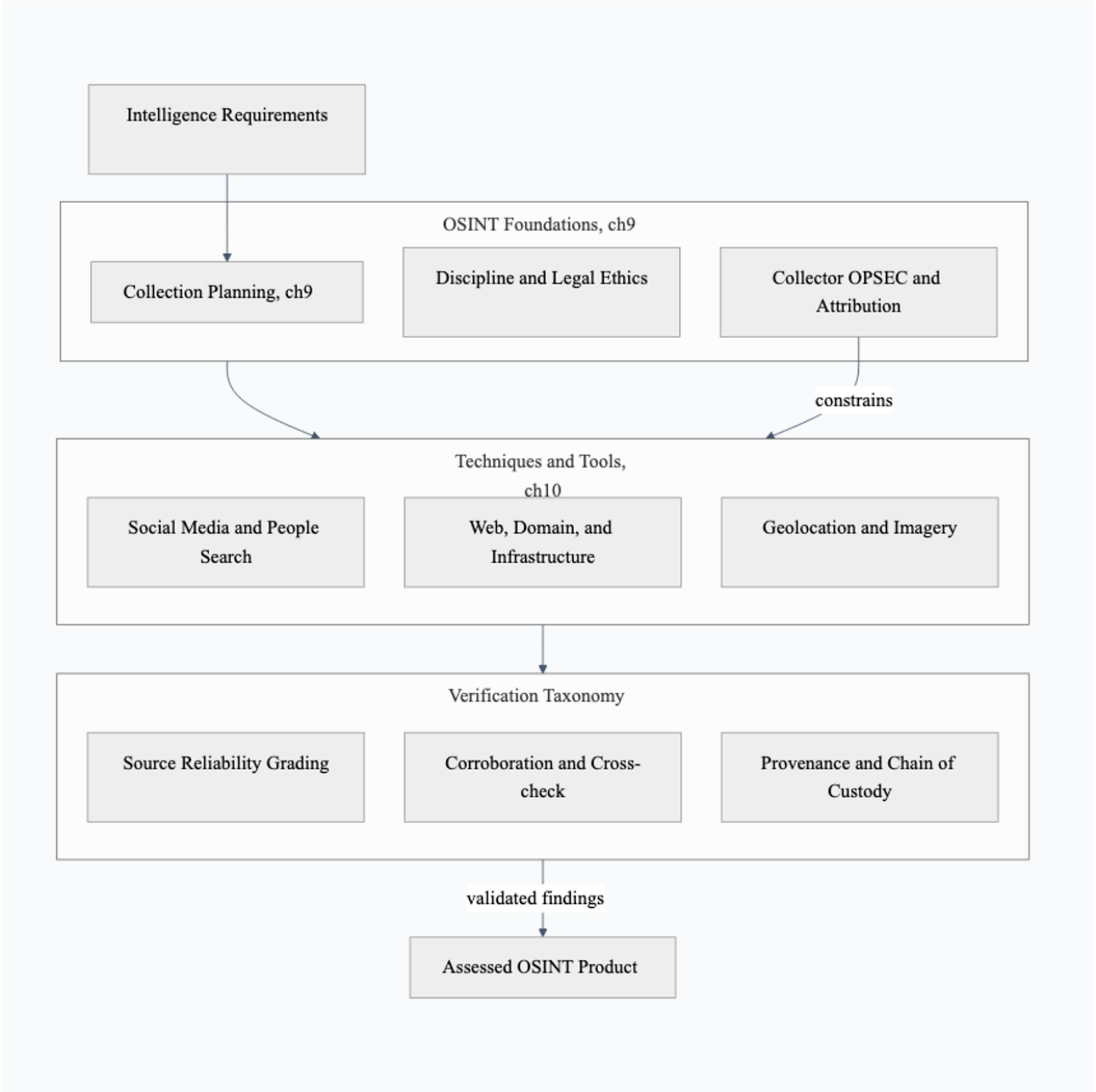


Figure 46: Part IV traces OSINT as a left-to-right pipeline from requirements through disciplined collection (ch9) and tooling (ch10) into a verification taxonomy that turns raw findings into an assessed product. Its reader value is to make Intelligence Requirements, Collection Planning, ch9, the module, ch9, and Discipline and Legal Ethics visible at a glance, with the open source intelligence osint section as the source section and defensive review as the boundary.

16 OSINT Foundations

16.0.1 OSINT Foundations figures and course links: visual evidence, source flow, and navigation

The module uses Figure 47 and Figure 45 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 15, Section 17.
This module teaches the **Open-Source and Geospatial Intelligence Integrity** lane through a bounded, source-backed coursebook chapter. [251, 2026]; [253, 2026].

16.1 Open-Source and Geospatial Intelligence Integrity frame for OSINT Foundations: source context, topic focus, and reader task

Evidence anchor. Section 16; [251, 2026].

16.1.1 OSINT Foundations orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 16; [251, 2026].

16.1.2 OSINT Foundations conceptual primer: source context, core model, and reader task

This chapter teaches OSINT and GEOINT as public-source reasoning disciplines: availability does not equal reliability, relevance, legality, or ethical reuse. The chapter uses **Requirements-to-Evidence Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**.
The central distinction is to separate discovery from collection expansion, and map or media interpretation from targeting. Core topics include **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026; OSINT vs. HUMINT vs. SIGINT: Comparative Value and Fusion**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [251, 2026]; [253, 2026].
Learners move from vocabulary and the **Requirements-to-Evidence Lens** distinction through topic lessons on **History and Rise of OSINT in the Intelligence Community** with evidence and misconception checks, then assemble a **requirements matrix with source descriptors, caveats, and collection limits** with safety and rights gates.

16.1.3 OSINT Foundations learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 16; [251, 2026].

- Connect **History and Rise of OSINT in the Intelligence Community and IC OSINT Strategy 2024–2026** to **Open-Source and Geospatial Intelligence Integrity** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **requirements matrix with source descriptors, caveats, and collection limits** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate discovery from collection expansion, and map or media interpretation from targeting; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as privacy drift, stale data, context collapse, platform bias, over-collection, and mistaking availability for reliability, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: OSINT work uses lawful public, owned-lab, or explicitly approved sources and avoids doxxing, harassment, live tracking, or operational targeting.

16.1.4 OSINT Foundations core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 16; [251, 2026].

Term	Working definition
Provenance	the origin, chain, and transformation history of a source
Corroboration	the comparison of independent sources before reuse
Recency	the time relationship between source creation, discovery, and claim
Geospatial quality	accuracy, completeness, temporal fitness, and usability of location data
Minimization	limiting retained information to what the accountable question requires
History and Rise of OSINT in the Intelligence…	Key terms: History, Rise, OSINT.
IC OSINT Strategy 2024–2026	Key terms: IC, OSINT, Strategy.

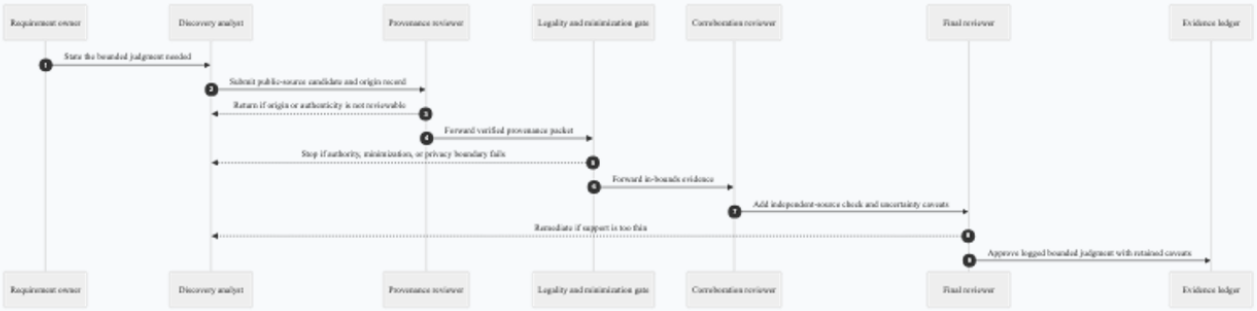


Figure 47: The OSINT sequence separates public-source discovery from claim reuse: each handoff records provenance, legality, minimization, corroboration, caveats, and reviewer disposition before a bounded judgment can be logged. In the open source intelligence osint / osint foundations section, it lets readers compare requirement owner, discovery analyst, provenance reviewer, legal and minimization gate, corroboration reviewer, final reviewer, logged bounded judgment, stop-and-retire path for unverifiable or out-of-bounds evidence so the visual functions as a traceable course aid rather than an unscoped assertion.

16.2 Requirements-to-Evidence Lens path for OSINT Foundations: lesson cluster, safe artifact, and review

Evidence anchor. Section 16; [251, 2026].

16.2.1 OSINT Foundations practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 16; [251, 2026].

16.2.2 OSINT Foundations topic lessons: source-backed concepts and transfer tasks

This module builds OSINT and GEOINT as public-source reasoning disciplines: availability does not equal reliability, relevance, legality, or ethical reuse. The sequence opens with **History and Rise of OSINT in the Intelligence Community**, **IC OSINT Strategy 2024–2026**, **OSINT vs. HUMINT vs. SIGINT: Comparative Value and Fusion** and applies the **Requirements-to-Evidence Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 45; module overview Section 16; curriculum atlas Section 2.

Triangulation anchors. In module 9's topic-lessons section, directly verified anchors for the **Open-Source and Geospatial Intelligence Integrity** lane include [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]; [Agency, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

16.2.2.1 Lesson 1: History and Rise of OSINT in the Intelligence Community

Concept. **History and Rise of OSINT in the Intelligence Community** maps the theory to institutions: priorities, feedback, incentives, review loops, and records shape what an intelligence community notices and ignores.

Why it matters. **History and Rise of OSINT in the Intelligence Community** connects classroom vocabulary to Open-Source and Geospatial Intelligence Integrity practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. **History and Rise of OSINT in the Intelligence Community** rests on [047, 2026]. The lead source's own note reads: Plans and strategies for improving open-source intelligence (OSINT) operations in the Intelligence. Use it for the working definition that **History and Rise of OSINT in the Intelligence Community** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. Ground **History and Rise of OSINT in the Intelligence Community** in the evidence the row cites. [047, 2026] Plans and strategies for improving open-source intelligence (OSINT) operations in the Intelligence. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **History and Rise of OSINT in the Intelligence Community**, build an institutional feedback-loop map with incentives, review points, and oversight hooks. Shape this subject work as an **OSINT provenance and minimization matrix** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that History and Rise of OSINT in the Intelligence Community can be used while ignoring the rule to separate discovery from collection expansion, and map or media interpretation from targeting.

Transfer task. Transfer **History and Rise of OSINT in the Intelligence Community** to a second module by preserving source-quality review and non-sensitive geospatial interpretation, changing the source evidence, and naming a new reviewer.

16.2.2.2 Lesson 2: IC OSINT Strategy 2024–2026

Concept. **IC OSINT Strategy 2024–2026** treats open sources as publicly available evidence that still requires provenance, corroboration, legality, and minimization before reuse.

Why it matters. **IC OSINT Strategy 2024–2026** matters in the **Open-Source and Geospatial Intelligence Integrity** lane because source-quality review and non-sensitive geospatial interpretation evidence must stay separate from judgment; privacy drift is a common failure.

Source support. **IC OSINT Strategy 2024–2026** rests on [048, 2026]. The lead source's own note reads: Tradecraft and training standards must be flexible and updated regularly to keep pace with changes. Use it for pinning down the scope of **IC OSINT Strategy 2024–2026**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. For **IC OSINT Strategy 2024–2026**, reason from the sources cited in this row. [048, 2026] Tradecraft and training standards must be flexible and updated regularly to keep pace with changes. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **IC OSINT Strategy 2024–2026**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this source-quality review and non-sensitive geospatial interpretation topic. The artifact must name the source descriptor, the bounded claim about **IC OSINT Strategy**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape this subject work as an **OSINT provenance and minimization matrix** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that IC OSINT Strategy 2024–2026 is optional whenever separate discovery from collection expansion, and map or media interpretation from targeting feels inconvenient.

Transfer task. Transfer **IC OSINT Strategy 2024–2026** to a second module by preserving source-quality review and non-sensitive geospatial interpretation, changing the source evidence, and naming a new reviewer.

16.2.2.3 Lesson 3: OSINT vs. HUMINT vs. SIGINT: Comparative Value and Fusion

Concept. **OSINT vs. HUMINT vs. SIGINT: Comparative Value and Fusion** treats human-source work as a governed relationship: validation, consent, reporting, source protection, and oversight—not contact activity.

Why it matters. **OSINT vs. HUMINT vs. SIGINT** connects classroom vocabulary to Open-Source and Geospatial Intelligence Integrity practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. **OSINT vs. HUMINT vs. SIGINT: Comparative Value and Fusion** rests on [301, 2026] and [298, 2026]. The most specific cited work observes: Official Intelligence Community strategy for open-source intelligence governance, integration, source discovery, data, tools, tradecraft, and workforce priorities. Use them for the claim that **OSINT vs. HUMINT vs. SIGINT: Comparative Value and Fusion** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. Read **OSINT vs. HUMINT vs. SIGINT** against the works cited for this row. [301, 2026] Official Intelligence Community strategy for open-source intelligence governance, integration, source discovery, data, tools, tradecraft, and workforce priorities. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **OSINT vs. HUMINT vs. SIGINT**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this source-quality review and non-sensitive geospatial interpretation topic. The artifact must name the source descriptor, the bounded claim about **OSINT vs HUMINT vs SIGINT**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **OSINT vs. HUMINT vs. SIGINT** work as an **OSINT provenance and minimization matrix** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that OSINT vs. HUMINT vs. SIGINT: Comparative Value and Fusion establishes intent without reviewing alternative explanations.

Transfer task. Transfer **OSINT vs. HUMINT vs. SIGINT** to a second module by preserving source-quality review and non-sensitive geospatial interpretation, changing the source evidence, and naming a new reviewer.

16.2.2.4 Lesson 4: Legal and Ethical Constraints in OSINT Collection

Concept. Legal and Ethical Constraints in OSINT Collection treats open sources as publicly available evidence that still requires provenance, corroboration, legality, and minimization before reuse.

Why it matters. Legal and Ethical Constraints in OSINT Collection matters in the **Open-Source and Geospatial Intelligence Integrity** lane because source-quality review and non-sensitive geospatial interpretation evidence must stay separate from judgment; privacy drift is a common failure.

Source support. Legal and Ethical Constraints in OSINT Collection rests on [298, 2026] and [297, 2026]. The most specific cited work observes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for pinning down the scope of **Legal and Ethical Constraints in OSINT Collection**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. Read **Legal and Ethical Constraints in OSINT Collection** against the works cited for this row. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Legal and Ethical Constraints in OSINT Collection**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this source-quality review and non-sensitive geospatial interpretation topic. The artifact must name the source descriptor, the bounded claim about **Legal and Ethical Constraints in**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape this subject work as an **OSINT provenance and minimization matrix** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that Legal and Ethical Constraints in OSINT Collection replaces human review whenever evidence looks plausible.

Transfer task. Transfer **Legal and Ethical Constraints in OSINT Collection** to a second module by preserving source-quality review and non-sensitive geospatial interpretation, changing the source evidence, and naming a new reviewer.

16.2.2.5 Lesson 5: Identity-and-provenance ethics audit with no impersonation

Concept. Identity-and-provenance ethics audit with no impersonation treats open sources as publicly available evidence that still requires provenance, corroboration, legality, and minimization before reuse.

Why it matters. Identity-and-provenance ethics audit connects classroom vocabulary to Open-Source and Geospatial Intelligence Integrity practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Identity-and-provenance ethics audit with no impersonation rests on [301, 2026] and [298, 2026]. Its anchor reference records: Official Intelligence Community strategy for open-source intelligence governance, integration, source discovery, data, tools, tradecraft, and workforce priorities. Use them for fixing what **Identity-and-provenance ethics audit with no impersonation** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. For **Identity-and-provenance ethics audit**, work from the cited evidence behind this row. [301, 2026] Official Intelligence Community strategy for open-source intelligence governance, integration, source discovery, data, tools, tradecraft, and workforce priorities. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Identity-and-provenance ethics audit**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this source-quality review and non-sensitive geospatial interpretation topic. The artifact must state the identity descriptor, the bounded claim about **Identity-and-provenance ethics audit**, the linkage caveat, the uncertainty note, the no-deanonymization boundary, and the reviewer who clears the record. Shape **Identity-and-provenance ethics audit** work as an **OSINT provenance and minimization matrix** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that a presented identity is an established one, when provenance requires tracing how that identity was created, verified, and could be forged.

Transfer task. Reuse the **Identity-and-provenance ethics audit** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

16.2.2.6 Lesson 6: Open Source Intelligence: Trends and Issues

Concept. Open Source Intelligence: Trends and Issues treats open sources as publicly available evidence that still requires provenance, corroboration, legality, and minimization before reuse.

Why it matters. Open Source Intelligence matters in the **Open-Source and Geospatial Intelligence Integrity** lane because source-quality review and non-sensitive geospatial interpretation evidence must stay separate from judgment; privacy drift is a common failure.

Source support. Open Source Intelligence: Trends and Issues rests on [049, 2026]. The closest source to this row notes: The text explores OSINT's advantages and disadvantages in intelligence activities. Use it for fixing what **Open Source Intelligence: Trends and Issues** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. Read **Open Source Intelligence** against the works cited for this row. [049, 2026] The text explores OSINT's advantages and disadvantages in intelligence activities. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Open Source Intelligence**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this source-quality review and non-sensitive geospatial interpretation topic. The artifact must name the source descriptor, the bounded claim about **Open Source Intelligence**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Open Source Intelligence** work as an **OSINT provenance and minimization matrix** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that Open Source Intelligence: Trends and Issues is optional whenever separate discovery from collection expansion, and map or media interpretation from targeting feels inconvenient.

Transfer task. Transfer **Open Source Intelligence** to a second module by preserving source-quality review and non-sensitive geospatial interpretation, changing the source evidence, and naming a new reviewer.

16.2.3 OSINT Foundations worked safe example: synthetic inputs, evidence, and review

Worked example: a synthetic public-resilience team checks whether open data supports a non-sensitive evacuation-route map. [251, 2026]; [253, 2026].

Triangulation anchors. In module 9's worked-example section, directly verified anchors for the **Open-Source and Geospatial Intelligence Integrity** lane include [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]; [Agency, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **open-source intelligence governance**. Learners use a **OSINT provenance and minimization matrix** and keep this boundary visible: No exposed-service lookup, credentialed access, identity exposure, doxxing, or live collection expansion.

Frame. The classroom question centers on **History and Rise of OSINT in the Intelligence Community**. Excluded actions stay explicit, and the **Requirements-to-Evidence Lens** planning question is: What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit?

Inputs. For the **History and Rise of OSINT in the Intelligence Community** scenario, use public road data, public weather notices, synthetic change examples, and instructor-provided metadata. The Requirements-to-Evidence Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **History and Rise of OSINT in the Intelligence Community**, students record provenance, test recency, compare independent sources, mark uncertainty, and remove unnecessary identity data. Pause whenever an inference about History and Rise of OSINT in the Intelligence Community appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **History and Rise of OSINT in the Intelligence Community** classroom scenario; unit artifact = OSINT provenance and minimization matrix; evidence = allowed inputs; method = source-quality review and non-sensitive geospatial interpretation; output = a source-quality matrix and annotated map note with caveats and no tracking or targeting content; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **History and Rise of OSINT in the Intelligence Community** as "Requirements-to-Evidence Lens confirms it" is not enough. The revision ties the claim to source-quality review and non-sensitive geospatial interpretation, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **History and Rise of OSINT in the Intelligence Community** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

16.2.4 OSINT Foundations practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Requirements-to-Evidence Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**.

Triangulation anchors. In module 9's practice-sequence section, directly verified anchors for the **Open-Source and Geospatial Intelligence Integrity** lane include [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]; [Agency, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare History and Rise of OSINT in the Intelligence Community, IC OSINT Strategy 2024–2026, OSINT vs. HUMINT vs. SIGINT: Comparative Value and Fusion; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Open-Source and Geospatial Intelligence Integrity** lane.
2. Frame	Answer the lens question: What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for History and Rise of OSINT in the Intelligence Community: requirements matrix with source descriptors, caveats, and collection limits.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the OSINT provenance and minimization matrix fields for History and Rise of OSINT in the Intelligence Community.	Unit profile note.	Evidence artifacts include provenance chain, terms-of-use note.
4. Challenge	Test the misconception that History and Rise of OSINT in the Intelligence Community can be used while ignoring the rule to separate discovery from collection expansion, and map or media interpretation from targeting.	Failure-mode note.	The artifact applies the key distinction: separate discovery from collection expansion, and map or media interpretation from targeting.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

16.2.4.1 OSINT Foundations instructor notes: source reasoning, review points, and studio focus

Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**. [251, 2026]; [253, 2026].

16.2.4.2 OSINT Foundations extension exercise: peer validation and refresh trigger review

Evidence anchor. Section 16; [251, 2026].

Have learners swap artifacts and apply the **Requirements-to-Evidence Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**.

16.2.5 OSINT Foundations knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 16; [251, 2026].

1. Explain how **History and Rise of OSINT in the Intelligence Community** is defined here; name the source descriptor that supports the definition.
2. Contrast **History and Rise of OSINT in the Intelligence Community** with **IC OSINT Strategy 2024–2026** using the **Requirements-to-Evidence Lens** artifact fields.
3. Identify one failure mode from the **Open-Source and Geospatial Intelligence Integrity** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which source is available but not reliable enough for the claim?
5. Correct this misconception: that History and Rise of OSINT in the Intelligence Community can be used while ignoring the rule to separate discovery from collection expansion, and map or media interpretation from targeting.

16.2.5.1 OSINT Foundations answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **History and Rise of OSINT in the Intelligence Community** without source evidence, uncertainty, or a safe transfer task.

16.3 OSINT Foundations assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 16; [251, 2026].

16.3.1 OSINT Foundations evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 16; [251, 2026].

16.3.2 OSINT Foundations transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 16; [251, 2026].

16.3.2.1 OSINT Foundations lineage and source tradition: profile, concepts, and first anchors This sits in the **Open-Source and Geospatial Intelligence Integrity** lineage: public-source discovery converted into accountable intelligence through provenance, corroboration, minimization, and relevance tests. [251, 2026]; [253, 2026].

16.3.2.2 OSINT Foundations working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 16; [251, 2026].
The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**, with provenance and reviewability throughout.

16.3.2.3 OSINT Foundations knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [251, 2026]; [253, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

16.3.2.4 OSINT Foundations transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 16; [251, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**.
- **Evidence contract:** keep the **Open-Source and Geospatial Intelligence Integrity** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

16.3.2.5 OSINT Foundations profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 16; [251, 2026].
The matched profile emphasizes public-source discovery converted into accountable intelligence through provenance, corroboration, minimization, and relevance tests. The method stack is source triage, provenance capture, corroboration matrix, recency audit, geospatial context review, and confidence calibration; the local topic cluster is **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**.

16.3.3 OSINT Foundations evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 16; [251, 2026].
Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Open-Source and Geospatial Intelligence Integrity** profile tells reviewers what evidence is strong enough for the module artifact built around **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**.

16.3.3.1 OSINT Foundations guide source spine: inherited keys and local citation roles Primary guide citations: [251, 2026]; [253, 2026]; [269, 2026]; [273, 2026]; [274, 2026]; [275, 2026]; [286, 2026]; [287, 2026]; [292, 2026]; [047, 2026]; [048, 2026]; [049, 2026]; [301, 2026]; [298, 2026]; [297, 2026].

16.3.3.2 OSINT Foundations verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [251, 2026]; [253, 2026].

Tier	What counts	How it is used
Source guide	[251, 2026]; [253, 2026]; [269, 2026]; [273, 2026]; [274, 2026]; [275, 2026]; [286, 2026]; [287, 2026]; [292, 2026]; [047, 2026]; [048, 2026]; [049, 2026]; [301, 2026]; [298, 2026]; [297, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 9's source-canon section, directly verified anchors for the **Open-Source and Geospatial Intelligence Integrity** lane include [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]; [Agency, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Maintenance rule: Perplexity may suggest candidates for **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026** and [251, 2026]; [253, 2026], but only directly verified source URLs are encoded as citations.

16.3.3.3 OSINT Foundations intelligence practice lens: evidence artifact and safety check Practice lens: **Requirements-to-Evidence Lens** for **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**. [251, 2026]; [253, 2026].
Planning question: What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit?
Evidence artifact: requirements matrix with source descriptors, caveats, and collection limits.
Validation rule: show priority, authority, minimization, corroboration, and source quality before any claim is reused. Applied to **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**.
Handoff contract: deliver metadata-rich evidence packets, not unscoped data piles or implicit targeting requests.
Safety check: exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure.

16.3.3.4 OSINT Foundations runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 16; [251, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	9.99	9.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind OSINT Foundations to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Bounded autonomy, procurement, incident-response, and assurance studio	9.101	9.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for OSINT Foundations	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Model-card, recoverability, retention, and learner-support evidence package	9.102	9.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for OSINT Foundations	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
History and Rise of OSINT in the Intelligence Community	9.1	9.1 History and Rise of OSINT in the Intelligence Community	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
IC OSINT Strategy 2024–2026	9.2	9.2 IC OSINT Strategy 2024–2026	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
OSINT vs. HUMINT vs. SIGINT: Comparative Value and Fusion	9.3	9.3 OSINT vs. HUMINT vs. SIGINT: Comparative Value and Fusion	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Legal and Ethical Constraints in OSINT Collection	9.4	9.4 Legal and Ethical Constraints in OSINT Collection	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Identity-and-provenance ethics audit with no impersonation	9.5	9.5 source title transformed into safe curriculum treatment; original: OPSEC for OSINT Operators: The Sock Puppet Problem	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Open Source Intelligence: Trends and Issues	9.6	9.6 Open Source Intelligence: Trends and Issues	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

16.3.3.5 OSINT Foundations reusable subsection contract: topic rows, artifacts, and safety duties **Evidence anchor.** Section 16; [251, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
History and Rise of OSINT in the Intelligence Community	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
IC OSINT Strategy 2024–2026	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
OSINT vs. HUMINT vs. SIGINT: Comparative Value and Fusion	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Legal and Ethical Constraints in OSINT Collection	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Identity-and-provenance ethics audit with no impersonation	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Open Source Intelligence: Trends and Issues	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

16.3.3.6 OSINT Foundations annotated source ledger: real titles and local contribution Each source cited by this **Open-Source and Geospatial Intelligence Integrity** module is paired below with its real title and a one-line note on what it contributes to **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**.

Source	Cited work	What it contributes	Status
[251, 2026]	European Data Governance Act	The European Commission page explaining the Data Governance Act, an EU regulation that became applicable in September 2023 to build trust in data sharing and ease reuse of data. It outlines four mechanisms: facilitating reuse of protected public-sector data, establishing trusted data intermediaries, enabling voluntary data sharing by citizens and businesses, and removing barriers to cross-sector and cross-border data use.	verified source-guide

Source	Cited work	What it contributes	Status
[253, 2026]	Common European Data Spaces	This is an official European Commission webpage describing the Common European Data Spaces initiative, part of the EU strategy to create interconnected, trustworthy data-sharing environments across strategic sectors. It explains that data spaces let organizations and individuals share data while retaining control, guided by principles of open participation, privacy protection, and fair access rules.	verified source-guide
[269, 2026]	Data on the Web Best Practices	A W3C Recommendation, "Data on the Web Best Practices," published January 31, 2017 by the Data on the Web Best Practices Working Group. It offers 35 best practices for publishing and consuming data on the Web, covering metadata, licensing and provenance, data quality, dataset versioning, persistent URIs, machine-readable formats, vocabulary reuse, access methods, preservation, and feedback.	verified source-guide
[273, 2026]	WCAG 2 Overview	The W3C Web Accessibility Initiative overview of the Web Content Accessibility Guidelines (WCAG), an international standard for making web content accessible to people with disabilities. It explains that WCAG is organized around four principles (perceivable, operable, understandable, robust) with testable success criteria at three conformance levels (A, AA, AAA), and covers versions 2.0, 2.1, and 2.2.	verified source-guide
[274, 2026]	CAST Universal Design for Learning Guidelines version 3.0	The official CAST website for the Universal Design for Learning (UDL) Guidelines version 3.0, released in 2024. The framework offers research-based guidance for designing inclusive learning environments and is organized around three principles: Engagement (motivation and emotional support), Representation (accessible presentation of information), and Action and Expression (diverse means of participation and communication).	verified source-guide
[275, 2026]	Fact Sheet: New Rule on the Accessibility of Web Content and Mobile Apps Provided by State and Local Governments	A US Department of Justice fact sheet explaining the 2024 ADA Title II rule requiring state and local governments to make their web content and mobile apps accessible. It establishes WCAG 2.1 Level AA as the technical standard, applies to entities such as schools, courts, libraries, and transit agencies, and sets compliance deadlines of April 2027 for larger jurisdictions and April 2028 for smaller ones.	verified source-guide

Source	Cited work	What it contributes	Status
[286, 2026]	Model Cards for Model Reporting	The arXiv abstract for "Model Cards for Model Reporting" (2018) by Mitchell, Wu, Zaldivar, and colleagues, which introduces a framework for transparent documentation of machine learning models. Model cards are short accompanying documents that report a model's benchmarked performance across varied conditions, including different cultural, demographic, and phenotypic groups, along with intended use, evaluation methodology, and deployment considerations.	verified source-guide
[287, 2026]	Datasheets for Datasets	A 2018 arXiv paper proposing 'datasheets for datasets,' a standardized documentation framework for machine learning datasets modeled on electronic component datasheets. The authors argue the field lacks consistent dataset documentation, which creates risk in high-stakes applications, and propose that datasets be accompanied by documentation covering motivation, composition, collection process, recommended uses, and test results.	verified source-guide
[292, 2026]	Assessing Risks and Impacts of AI (ARIA): Pilot Evaluation Report	The ARIA 0.1 pilot evaluation report documents NIST's methodology for systematically assessing AI applications for risks and societal impacts, using a multi-layered evaluation approach across five participating organizations and seven submitted AI applications. The pilot employed three evaluation scenarios and three testing levels: model testing, red teaming, and field testing, supplemented by dialogue annotation, tester questionnaires, and structured measurement trees.	verified source-guide
[047, 2026]	How the Intelligence Community Has Held Back Open-Source	Plans and strategies for improving open-source intelligence (OSINT) operations in the Intelligence.	original source-guide
[048, 2026]	The IC OSINT Strategy 2024-2026	Tradecraft and training standards must be flexible and updated regularly to keep pace with changes.	original source-guide
[049, 2026]	Open Source Intelligence (OSINT): issues and trends	The text explores OSINT's advantages and disadvantages in intelligence activities.	original source-guide
[301, 2026]	The IC OSINT Strategy 2024-2026	Official Intelligence Community strategy for open-source intelligence governance, integration, source discovery, data, tools, tradecraft, and workforce priorities.	original source-guide
[298, 2026]	Intelligence Community Directives	Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations.	original source-guide
[297, 2026]	Intelligence Community Directive 203: Analytic Standards	Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products.	original source-guide

Where this sits. This module's overview is Section 16; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

16.3.4 OSINT Foundations governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 16; [251, 2026].

16.3.5 OSINT Foundations analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 9's governance-boundary section, directly verified anchors for the **Open-Source and Geospatial Intelligence Integrity** lane include [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]; [Agency, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Research lane: **Open-Source and Geospatial Intelligence Integrity** for **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**. [251, 2026]; [253, 2026].
Curriculum topic spine: History and Rise of OSINT in the Intelligence Community, **IC OSINT Strategy 2024–2026**, **OSINT vs. HUMINT vs. SIGINT: Comparative Value and Fusion**. **Verified anchor cluster:** [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]; [Agency, 2026b]; [for Standardization, 2013]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015].
Conceptual depth: public-source discovery converted into accountable intelligence through provenance, corroboration, minimization, and relevance tests.
Method stack: source triage, provenance capture, corroboration matrix, recency audit, geospatial context review, and confidence calibration.
Composability contract: collection notes, source metadata, transformations, caveats, and analytic judgments remain separately exportable.
Known failure modes: privacy drift, stale data, context collapse, platform bias, over-collection, and mistaking availability for reliability.
Defensive boundary: OSINT work uses lawful public, owned-lab, or explicitly approved sources and avoids doxxing, harassment, live tracking, or operational targeting. Applied to **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**.

Anchor	Why it matters here
[of the Director of National Intelligence and Agency, 2024]	Official IC OSINT strategy for professionalizing OSINT, integrated collection management, open-source sharing, innovation, and tradecraft. Checked as of 2026-05-21; role: curriculum_anchor.
[of State, 2024]	Official strategy source for lawful OSINT governance, discovery, validation, and dissemination. Checked as of 2026-05-21; role: curriculum_anchor.
[Agency, 2026c]	Official NGA strategy anchor for GEOINT readiness, warning, partnership resilience, resource stewardship, and AI integration. Checked as of 2026-05-21; role: curriculum_anchor.
[Agency, 2026b]	Official NGA source on GEOINT AI, data quality, model performance, interoperability, analyst interaction, and standards leadership. Checked as of 2026-05-21; role: curriculum_anchor.
[for Standardization, 2013]	International geospatial data-quality standard for completeness, logical consistency, positional accuracy, temporal quality, and usability framing. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026d]	Official sourcing directive for traceability, citations, source descriptors, and source summaries. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2015]	Official ODNI analytic tradecraft standards directive. Checked as of 2026-05-21; role: source_quality_anchor.

16.3.5.1 OSINT Foundations evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **Open-Source and Geospatial Intelligence Integrity** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [251, 2026]; [253, 2026].

16.3.6 OSINT Foundations agentic boundary: assist, approve, block, and record

Evidence anchor. Section 16; [251, 2026].
AGEINT translation is bounded by the **Open-Source and Geospatial Intelligence Integrity** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**.

16.3.6.1 OSINT Foundations permitted defensive utility: curriculum uses and safe outputs

Evidence anchor. Section 16; [251, 2026].
The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**.

16.3.6.2 OSINT Foundations excluded operational boundary: blocked actions and stop rules

Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [251, 2026]; [253, 2026] and **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

16.3.7 OSINT Foundations governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 16; [251, 2026].
Governance is practiced as a gate on the **Open-Source and Geospatial Intelligence Integrity** lane. Learners use the **Requirements-to-Evidence Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**.

16.3.7.1 OSINT Foundations governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [251, 2026]; [253, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Open-Source and Geospatial Intelligence Integrity** failure modes and the **Requirements-to-Evidence Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

16.3.7.2 OSINT Foundations evidence package handoff: appendices, records, and reuse **Evidence anchor.** Section 16; [251, 2026]. Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Requirements-to-Evidence Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**.

16.3.7.3 OSINT Foundations current-source assurance: verified anchors and local artifact fit The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**. [251, 2026]; [253, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_ic_osint_strategy` for **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**?	The INT of First Resort: The IC OSINT Strategy 2024-2026; lane `osint_geoint`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official IC OSINT strategy for professionalizing OSINT, integrated collection management, open-source sharing, innovation, and tradecraft.
What does the module inherit from `official_state_osint_strategy` for **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**?	Open Source Intelligence Strategy; lane `osint_geoint`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official strategy source for lawful OSINT governance, discovery, validation, and dissemination.
What does the module inherit from `official_nga_strategy` for **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**?	NGA Strategy; lane `osint_geoint`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official NGA strategy anchor for GEOINT readiness, warning, partnership resilience, resource stewardship, and AI integration.
What does the module inherit from `official_nga_geoint_ai` for **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**?	GEOINT Artificial Intelligence; lane `osint_geoint`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official NGA source on GEOINT AI, data quality, model performance, interoperability, analyst interaction, and standards leadership.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 16; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

16.3.8 OSINT Foundations assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 16; [251, 2026].

16.3.9 OSINT Foundations assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 16; [251, 2026].

16.3.9.1 OSINT Foundations capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**.
Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026** and [251, 2026]; [253, 2026].

16.3.9.2 OSINT Foundations instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026** and [251, 2026]; [253, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

16.3.9.3 OSINT Foundations assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
History and Rise of OSINT in the Intelligence Community	Completed **requirements matrix with source descriptors, caveats, and collection limits** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
IC OSINT Strategy 2024–2026	Completed **requirements matrix with source descriptors, caveats, and collection limits** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
OSINT vs. HUMINT vs. SIGINT: Comparative Value and Fusion	Completed **requirements matrix with source descriptors, caveats, and collection limits** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

16.3.10 OSINT Foundations refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [251, 2026]; [253, 2026] and **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**.

16.3.10.1 OSINT Foundations refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**. The local signals begin with [251, 2026]; [253, 2026].

16.3.10.2 OSINT Foundations claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**, and the source spine for these checks begins with [251, 2026]; [253, 2026].

16.3.11 OSINT Foundations reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [251, 2026]; [253, 2026].
Triangulation anchors. In module 9's review-checklist section, directly verified anchors for the **Open-Source and Geospatial Intelligence Integrity** lane include [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]; [Agency, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026**. [251, 2026]; [253, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

16.3.12 OSINT Foundations learning-path links: module map, overview, and curriculum atlas

Use the cross-links below to place **History and Rise of OSINT in the Intelligence Community; IC OSINT Strategy 2024–2026** in the wider unit: the orientation sets the frame, the parent unit supplies the shared safety posture, and the neighbouring modules show what evidence enters and leaves. Lead sources: [251, 2026]; [253, 2026].
Section 2, Section 15, Section 17

17 OSINT Techniques and Tools

17.0.1 OSINT Techniques and Tools figures and course links: visual evidence, source flow, and navigation

The module uses Figure 48 and Figure 45 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 15, Section 16, Section 18.
This module teaches the **Open-Source and Geospatial Intelligence Integrity** lane through a bounded, source-backed coursebook chapter. [251, 2026]; [252, 2026].

17.1 Open-Source and Geospatial Intelligence Integrity frame for OSINT Techniques and Tools: source context, topic focus, and reader task

Evidence anchor. Section 17; [251, 2026].

17.1.1 OSINT Techniques and Tools orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 17; [251, 2026].

17.1.2 OSINT Techniques and Tools conceptual primer: source context, core model, and reader task

This chapter teaches OSINT and GEOINT as public-source reasoning disciplines: availability does not equal reliability, relevance, legality, or ethical reuse. The chapter uses **Requirements-to-Evidence Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records**.
The central distinction is to separate discovery from collection expansion, and map or media interpretation from targeting. Core topics include **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records; Graph-analysis provenance review using instructor-provided records**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [251, 2026]; [252, 2026].
Learners move from vocabulary and the **Requirements-to-Evidence Lens** distinction through topic lessons on **Search-exposure provenance review using instructor-provided records** with evidence and misconception checks, then assemble a **requirements matrix with source descriptors, caveats, and collection limits** with safety and rights gates.

17.1.3 OSINT Techniques and Tools learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 17; [251, 2026].

- Connect **Search-exposure provenance review using instructor-provided records and Social-source provenance and minimization review using toy records** to **Open-Source and Geospatial Intelligence Integrity** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **requirements matrix with source descriptors, caveats, and collection limits** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate discovery from collection expansion, and map or media interpretation from targeting; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as privacy drift, stale data, context collapse, platform bias, over-collection, and mistaking availability for reliability, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: OSINT work uses lawful public, owned-lab, or explicitly approved sources and avoids doxxing, harassment, live tracking, or operational targeting.

17.1.4 OSINT Techniques and Tools core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 17; [251, 2026].

Term	Working definition
Provenance	the origin, chain, and transformation history of a source
Corroboration	the comparison of independent sources before reuse
Recency	the time relationship between source creation, discovery, and claim
Geospatial quality	accuracy, completeness, temporal fitness, and usability of location data
Minimization	limiting retained information to what the accountable question requires
Search-exposure provenance review using…	Key terms: Search, exposure, provenance.
Social-source provenance and minimization…	Key terms: Social, provenance, minimization.

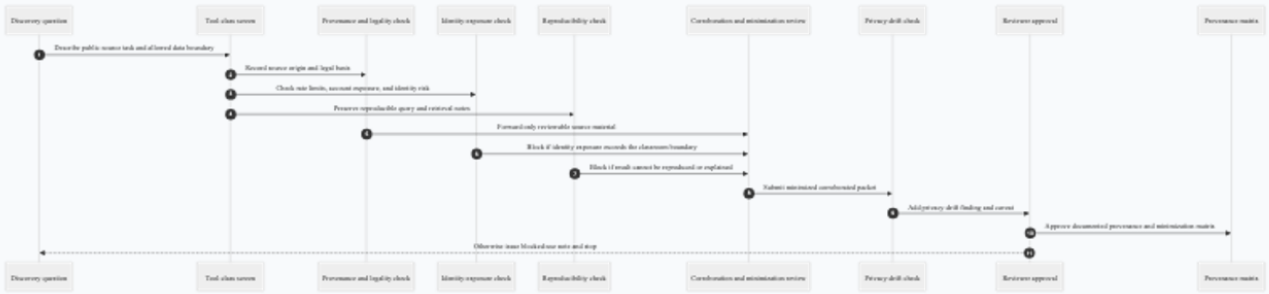


Figure 48: The OSINT provenance sequence makes the governance screen explicit: tool class, provenance, legality, identity exposure, reproducibility, minimization, privacy drift, and reviewer approval are checked before reuse. The captioned view belongs to the open source intelligence osint / osint techniques and tools section and should be read as a map of public-source question, tool-class governance screen, provenance and legality check, identity-exposure check, reproducibility check, corroboration and minimization review, privacy-drift check, reviewer approval, documented matrix or blocked-use note, not as a capability score or live-task instruction.

17.2 Requirements-to-Evidence Lens path for OSINT Techniques and Tools: lesson cluster, safe artifact, and review

Evidence anchor. Section 17; [251, 2026].

17.2.1 OSINT Techniques and Tools practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 17; [251, 2026].

17.2.2 OSINT Techniques and Tools topic lessons: source-backed concepts and transfer tasks

This module builds OSINT and GEOINT as public-source reasoning disciplines: availability does not equal reliability, relevance, legality, or ethical reuse. The sequence opens with **Search-exposure provenance review using instructor-provided records**, **Social-source provenance and minimization review using toy records**, **Graph-analysis provenance review using instructor-provided records** and applies the **Requirements-to-Evidence Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 45; module overview Section 17; curriculum atlas Section 2.

Triangulation anchors. In module 10's topic-lessons section, directly verified anchors for the **Open-Source and Geospatial Intelligence Integrity** lane include [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]; [Agency, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

17.2.2.1 Lesson 1: Search-exposure provenance review using instructor-provided records

Concept. Search-exposure provenance review using instructor-provided records evaluates the tool class by provenance, legality, rate limits, identity exposure, and reproducibility before any public-source claim is reused.

Why it matters. Analysts use **Search-exposure provenance review** to separate discovery from collection expansion, and map or media interpretation from targeting. A defensible treatment names the judgment it enables for source-quality review and non-sensitive geospatial interpretation review, the proof limit that privacy drift would otherwise hide, and the reviewer accountable for challenge.

Source support. Search-exposure provenance review using instructor-provided records rests on [050, 2026] and [051, 2026]. The most specific cited work observes: Mike wrote he wants to make the OSINT investigator more self reliant, able to do his job without. Use them for pinning down the scope of **Search-exposure provenance review using instructor-provided records**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. Read **Search-exposure provenance review** against the works cited for this row. [050, 2026] Mike wrote he wants to make the OSINT investigator more self reliant, able to do his job without. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Search-exposure provenance review**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this source-quality review and non-sensitive geospatial interpretation topic. The artifact must record the tool-and-terms descriptor, the bounded claim about **Search-exposure provenance review using instructor-provided**, the minimization caveat, the reproducibility uncertainty, the identity-exposure boundary, and the reviewer who approves the use. Shape **Search-exposure provenance review** work as an **OSINT provenance and minimization matrix** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Search-exposure provenance review**: that a source being publicly accessible means collecting it is unrestricted, ungoverned, and free of legal, ethical, and scoping limits.

Transfer task. Apply this module's safe boundary for **Search-exposure provenance review** to another artifact while keeping source-quality review and non-sensitive geospatial interpretation and reviewer ownership explicit.

17.2.2.2 Lesson 2: Social-source provenance and minimization review using toy records

Concept. Social-source provenance and minimization review using toy records treats open sources as publicly available evidence that still requires provenance, corroboration, legality, and minimization before reuse.

Why it matters. Social-source provenance matters in the **Open-Source and Geospatial Intelligence Integrity** lane because source-quality review and non-sensitive geospatial interpretation evidence must stay separate from judgment; privacy drift is a common failure.

Source support. Social-source provenance and minimization review using toy records rests on [051, 2026] and [052, 2026]. Its anchor reference records: This article defines open source intelligence as the practice of gathering information from publicly available data for security, business, and investigative purposes, drawing on websites, social media, government records, and public databases. Use them for fixing what **Social-source provenance and minimization review using toy records** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. For **Social-source provenance**, work from the cited evidence behind this row. [052, 2026] This article defines open source intelligence as the practice of gathering information from publicly available data for security, business, and investigative purposes, drawing on websites, social media, government records, and public databases. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Social-source provenance**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this source-quality review and non-sensitive geospatial interpretation topic. The artifact must record the tool-and-terms descriptor, the bounded claim about **Social-source provenance and minimization review**, the minimization caveat, the reproducibility uncertainty, the identity-exposure boundary, and the reviewer who approves the use. Shape **Social-source provenance** work as an **OSINT provenance and minimization matrix** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Social-source provenance**: that a source being publicly accessible means collecting it is unrestricted, ungoverned, and free of legal, ethical, and scoping limits.

Transfer task. Reuse the **Social-source provenance** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

17.2.2.3 Lesson 3: Graph-analysis provenance review using instructor-provided records

Concept. Graph-analysis provenance review using instructor-provided records treats open sources as publicly available evidence that still requires provenance, corroboration, legality, and minimization before reuse.

Why it matters. Graph-analysis provenance review connects classroom vocabulary to Open-Source and Geospatial Intelligence Integrity practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Graph-analysis provenance review using instructor-provided records rests on [051, 2026]. Use it for the claim that **Graph-analysis provenance review using instructor-provided records** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. For **Graph-analysis provenance review**, reason from the sources cited in this row. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Graph-analysis provenance review**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this source-quality review and non-sensitive geospatial interpretation topic. The artifact must record the tool-and-terms descriptor, the bounded claim about **Graph-analysis provenance review using instructor-provided**, the minimization caveat, the reproducibility uncertainty, the identity-exposure boundary, and the reviewer who approves the use. Shape **Graph-analysis provenance review** work as an **OSINT provenance and minimization matrix** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Graph-analysis provenance review**: that a source being publicly accessible means collecting it is unrestricted, ungoverned, and free of legal, ethical, and scoping limits.

Transfer task. Transfer **Graph-analysis provenance review** from this module to a second motif by preserving source-quality review and non-sensitive geospatial interpretation, replacing action with audit, and naming the blocked use.

17.2.2.4 Lesson 4: Custom-source integration governance review using toy records

Concept. Custom-source integration governance review using toy records evaluates the tool class by provenance, legality, rate limits, identity exposure, and reproducibility before any public-source claim is reused.

Why it matters. Custom-source integration governance review connects classroom vocabulary to Open-Source and Geospatial Intelligence Integrity practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Custom-source integration governance review using toy records rests on [052, 2026] and [053, 2026]. The most specific cited work observes: This article defines open source intelligence as the practice of gathering information from publicly available data for security, business, and investigative purposes, drawing on websites, social media, government records, and public databases. Use them for pinning down the scope of **Custom-source integration governance review using toy records**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. Ground **Custom-source integration governance review** in the evidence the row cites. [052, 2026] This article defines open source intelligence as the practice of gathering information from publicly available data for security, business, and investigative purposes, drawing on websites, social media, government records, and public databases. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Custom-source integration governance review**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this source-quality review and non-sensitive geospatial interpretation topic. The artifact must record the tool-and-terms descriptor, the bounded claim about **Custom-source integration governance review using**, the minimization caveat, the reproducibility uncertainty, the identity-exposure boundary, and the reviewer who approves the use. Shape **Custom-source integration governance review** work as an **OSINT provenance and minimization matrix** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Custom-source integration governance review**: that a source being publicly accessible means collecting it is unrestricted, ungoverned, and free of legal, ethical, and scoping limits.

Transfer task. Transfer **Custom-source integration governance review** from this module to a second motif by preserving source-quality review and non-sensitive geospatial interpretation, replacing action with audit, and naming the blocked use.

17.2.2.5 Lesson 5: Automated-source aggregation governance review using toy records

Concept. Automated-source aggregation governance review using toy records treats open sources as publicly available evidence that still requires provenance, corroboration, legality, and minimization before reuse.

Why it matters. Without explicit treatment of **Automated-source aggregation governance review**, privacy drift undermines source-quality review and non-sensitive geospatial interpretation review; the lesson builds the habit to separate discovery from collection expansion, and map or media interpretation from targeting.

Source support. Automated-source aggregation governance review using toy records rests on [052, 2026]. Its anchor reference records: This article defines open source intelligence as the practice of gathering information from publicly available data for security, business, and investigative purposes, drawing on websites, social media, government records, and public databases. Use it for pinning down the scope of **Automated-source aggregation governance review using toy records**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. For **Automated-source aggregation governance review**, work from the cited evidence behind this row. [052, 2026] This article defines open source intelligence as the practice of gathering information from publicly available data for security, business, and investigative purposes, drawing on websites, social media, government records, and public databases. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Automated-source aggregation governance review**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this source-quality review and non-sensitive geospatial interpretation topic. The artifact must record the tool-and-terms descriptor, the bounded claim about **Automated-source aggregation governance review using**, the minimization caveat, the reproducibility uncertainty, the identity-exposure boundary, and the reviewer who approves the use. Shape **Automated-source aggregation governance review** work as an **OSINT provenance and minimization matrix** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Automated-source aggregation governance review**: that a source being publicly accessible means collecting it is unrestricted, ungoverned, and free of legal, ethical, and scoping limits.

Transfer task. Apply this module's safe boundary for **Automated-source aggregation governance review** to another artifact while keeping source-quality review and non-sensitive geospatial interpretation and reviewer ownership explicit.

17.2.2.6 Lesson 6: Identity-data minimization review using instructor-provided records

Concept. Identity-data minimization review using instructor-provided records evaluates the tool class by provenance, legality, rate limits, identity exposure, and reproducibility before any public-source claim is reused.

Why it matters. Analysts use **Identity-data minimization review** to separate discovery from collection expansion, and map or media interpretation from targeting. A defensible treatment names the judgment it enables for source-quality review and non-sensitive geospatial interpretation review, the proof limit that privacy drift would otherwise hide, and the reviewer accountable for challenge.

Source support. Identity-data minimization review using instructor-provided records rests on [054, 2026]. The closest source to this row notes: Top open source intelligence websites. Use it for the working definition that **Identity-data minimization review using instructor-provided records** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. For **Identity-data minimization review**, reason from the sources cited in this row. [054, 2026] Recommended OSINT tools and their benefits. Top open source intelligence websites. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Identity-data minimization review**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this source-quality review and non-sensitive geospatial interpretation topic. The artifact must record the tool-and-terms descriptor, the bounded claim about **Identity-data minimization review using instructor-provided**, the minimization caveat, the reproducibility uncertainty, the identity-exposure boundary, and the reviewer who approves the use. Shape **Identity-data minimization review** work as an **OSINT provenance and minimization matrix** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Identity-data minimization review**: that a source being publicly accessible means collecting it is unrestricted, ungoverned, and free of legal, ethical, and scoping limits.

Transfer task. Transfer **Identity-data minimization review** from this module to a second motif by preserving source-quality review and non-sensitive geospatial interpretation, replacing action with audit, and naming the blocked use.

17.2.2.7 Lesson 7: OSINT Framework (osintframework.com): Module Taxonomy Concept. OSINT Framework (osintframework.com): Module Taxonomy treats open sources as publicly available evidence that still requires provenance, corroboration, legality, and minimization before reuse.

Why it matters. OSINT Framework (osintframework.com) matters in the **Open-Source and Geospatial Intelligence Integrity** lane because source-quality review and non-sensitive geospatial interpretation evidence must stay separate from judgment; privacy drift is a common failure.

Source support. OSINT Framework (osintframework.com): Module Taxonomy rests on [051, 2026] and [052, 2026]. The closest source to this row notes: This article defines open source intelligence as the practice of gathering information from publicly available data for security, business, and investigative purposes, drawing on websites, social media, government records, and public databases. Use them for the claim that **OSINT Framework (osintframework.com): Module Taxonomy** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. For **OSINT Framework (osintframework.com)**, reason from the sources cited in this row. [052, 2026] This article defines open source intelligence as the practice of gathering information from publicly available data for security, business, and investigative purposes, drawing on websites, social media, government records, and public databases. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **OSINT Framework (osintframework.com)**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this source-quality review and non-sensitive geospatial interpretation topic. The artifact must name the source descriptor, the bounded claim about **OSINT Framework**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **OSINT Framework (osintframework.com)** work as an **OSINT provenance and minimization matrix** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that OSINT Framework (osintframework.com): Module Taxonomy is optional whenever separate discovery from collection expansion, and map or media interpretation from targeting feels inconvenient.

Transfer task. Transfer **OSINT Framework (osintframework.com)** to a second module by preserving source-quality review and non-sensitive geospatial interpretation, changing the source evidence, and naming a new reviewer.

17.2.2.8 Lesson 8: Offline OSINT Environments: VM Architecture and Isolation Concept. Offline OSINT Environments: VM Architecture and Isolation treats open sources as publicly available evidence that still requires provenance, corroboration, legality, and minimization before reuse.

Why it matters. Offline OSINT Environments connects classroom vocabulary to Open-Source and Geospatial Intelligence Integrity practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Offline OSINT Environments: VM Architecture and Isolation rests on [051, 2026] and [052, 2026]. The closest source to this row notes: This article defines open source intelligence as the practice of gathering information from publicly available data for security, business, and investigative purposes, drawing on websites, social media, government records, and public databases. Use them for the claim that **Offline OSINT Environments: VM Architecture and Isolation** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. For **Offline OSINT Environments**, reason from the sources cited in this row. [052, 2026] This article defines open source intelligence as the practice of gathering information from publicly available data for security, business, and investigative purposes, drawing on websites, social media, government records, and public databases. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Offline OSINT Environments**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this source-quality review and non-sensitive geospatial interpretation topic. The artifact must name the source descriptor, the bounded claim about **Offline OSINT Environments**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Offline OSINT Environments** work as an **OSINT provenance and minimization matrix** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that Offline OSINT Environments: VM Architecture and Isolation establishes intent without reviewing alternative explanations.

Transfer task. Transfer **Offline OSINT Environments** to a second module by preserving source-quality review and non-sensitive geospatial interpretation, changing the source evidence, and naming a new reviewer.

17.2.2.9 Lesson 9: IntelTechniques OSINT 11th Edition Methods and Workflows Concept. IntelTechniques OSINT 11th Edition Methods and Workflows treats open sources as publicly available evidence that still requires provenance, corroboration, legality, and minimization before reuse.

Why it matters. Without explicit treatment of **IntelTechniques OSINT 11th Edition Methods**, privacy drift undermines source-quality review and non-sensitive geospatial interpretation review; the lesson builds the habit to separate discovery from collection expansion, and map or media interpretation from targeting.

Source support. IntelTechniques OSINT 11th Edition Methods and Workflows rests on [055, 2026] and [056, 2026]. The lead source's own note reads: Resources for Uncovering Online Information - 11th Edition (2024). Use them for the claim that **IntelTechniques OSINT 11th Edition Methods and Workflows** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. For **IntelTechniques OSINT 11th Edition Methods**, reason from the sources cited in this row. [055, 2026] OSINT Techniques. Resources for Uncovering Online Information - 11th Edition (2024). [056, 2026] All tutorials in this book were confirmed accurate as of November 1, 2024. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **IntelTechniques OSINT 11th Edition Methods**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this source-quality review and non-sensitive geospatial interpretation topic. The artifact must name the source descriptor, the bounded claim about **IntelTechniques OSINT 11th Edition Methods**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **IntelTechniques OSINT 11th Edition Methods** work as an **OSINT provenance and minimization matrix** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that IntelTechniques OSINT 11th Edition Methods and Workflows replaces human review whenever evidence looks plausible.

Transfer task. Transfer **IntelTechniques OSINT 11th Edition Methods** to a second module by preserving source-quality review and non-sensitive geospatial interpretation, changing the source evidence, and naming a new reviewer.

17.2.3 OSINT Techniques and Tools worked safe example: synthetic inputs, evidence, and review

Worked example: a synthetic public-resilience team checks whether open data supports a non-sensitive evacuation-route map. [251, 2026]; [252, 2026].

Triangulation anchors. In module 10's worked-example section, directly verified anchors for the **Open-Source and Geospatial Intelligence Integrity** lane include [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]; [Agency, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **open-source intelligence governance**. Learners use a **OSINT provenance and minimization matrix** and keep this boundary visible: No exposed-service lookup, credentialed access, identity exposure, doxxing, or live collection expansion.

Frame. The classroom question centers on **Search-exposure provenance review using instructor-provided records**. Excluded actions stay explicit, and the **Requirements-to-Evidence Lens** planning question is: What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit?

Inputs. For the **Search-exposure provenance review using instructor-provided records** scenario, use public road data, public weather notices, synthetic change examples, and instructor-provided metadata. The Requirements-to-Evidence Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Search-exposure provenance review using instructor-provided records**, students record provenance, test recency, compare independent sources, mark uncertainty, and remove unnecessary identity data. Pause whenever an inference about Search-exposure provenance review using instructor-provided records appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Search-exposure provenance review using instructor-provided records** classroom scenario; unit artifact = OSINT provenance and minimization matrix; evidence = allowed inputs; method = source-quality review and non-sensitive geospatial interpretation; output = a source-quality matrix and annotated map note with caveats and no tracking or targeting content; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Search-exposure provenance review using instructor-provided records** as "Requirements-to-Evidence Lens confirms it" is not enough. The revision ties the claim to source-quality review and non-sensitive geospatial interpretation, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Search-exposure provenance review using instructor-provided records** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

17.2.4 OSINT Techniques and Tools practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Requirements-to-Evidence Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records**.

Triangulation anchors. In module 10's practice-sequence section, directly verified anchors for the **Open-Source and Geospatial Intelligence Integrity** lane include [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]; [Agency, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Search-exposure provenance review using instructor-provided records, Social-source provenance and minimization review using toy records, Graph-analysis provenance review using instructor-provided records; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Open-Source and Geospatial Intelligence Integrity** lane.
2. Frame	Answer the lens question: What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Search-exposure provenance review using instructor-provided records: requirements matrix with source descriptors, caveats, and collection limits.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the OSINT provenance and minimization matrix fields for Search-exposure provenance review using instructor-provided records.	Unit profile note.	Evidence artifacts include provenance chain, terms-of-use note.
4. Challenge	Test the misconception that a source being publicly accessible means collecting it is unrestricted, ungoverned, and free of legal, ethical, and scoping limits.	Failure-mode note.	The artifact applies the key distinction: separate discovery from collection expansion, and map or media interpretation from targeting.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

17.2.4.1 OSINT Techniques and Tools instructor notes: source reasoning, review points, and studio focus

Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records**. [251, 2026]; [252, 2026].

17.2.4.2 OSINT Techniques and Tools extension exercise: peer validation and refresh trigger review

Evidence anchor. Section 17; [251, 2026].

Have learners swap artifacts and apply the **Requirements-to-Evidence Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Search-exposure provenance review using instructor-provided records;**

Social-source provenance and minimization review using toy records.

17.2.5 OSINT Techniques and Tools knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 17; [251, 2026].

1. Explain how **Search-exposure provenance review using instructor-provided records** is defined here; name the source descriptor that supports the definition.
2. Contrast **Search-exposure provenance review using instructor-provided records** with **Social-source provenance and minimization review using toy records** using the **Requirements-to-Evidence Lens** artifact fields.
3. Identify one failure mode from the **Open-Source and Geospatial Intelligence Integrity** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which source is available but not reliable enough for the claim?
5. Correct this misconception: that a source being publicly accessible means collecting it is unrestricted, ungoverned, and free of legal, ethical, and scoping limits.

17.2.5.1 OSINT Techniques and Tools answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Search-exposure provenance review using instructor-provided records** without source evidence, uncertainty, or a safe transfer task.

17.3 OSINT Techniques and Tools assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 17; [251, 2026].

17.3.1 OSINT Techniques and Tools evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 17; [251, 2026].

17.3.2 OSINT Techniques and Tools transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 17; [251, 2026].

17.3.2.1 OSINT Techniques and Tools lineage and source tradition: profile, concepts, and first anchors This sits in the **Open-Source and Geospatial Intelligence Integrity** lineage: public-source discovery converted into accountable intelligence through provenance, corroboration, minimization, and relevance tests. [251, 2026]; [252, 2026].

17.3.2.2 OSINT Techniques and Tools working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 17; [251, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records**, with provenance and reviewability throughout.

17.3.2.3 OSINT Techniques and Tools knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [251, 2026]; [252, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

17.3.2.4 OSINT Techniques and Tools transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 17; [251, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records**.
- **Evidence contract:** keep the **Open-Source and Geospatial Intelligence Integrity** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

17.3.2.5 OSINT Techniques and Tools profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 17; [251, 2026].

The matched profile emphasizes public-source discovery converted into accountable intelligence through provenance, corroboration, minimization, and relevance tests. The method stack is source triage, provenance capture, corroboration matrix, recency audit, geospatial context review, and confidence calibration; the local topic cluster is **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records**.

17.3.3 OSINT Techniques and Tools evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 17; [251, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Open-Source and Geospatial Intelligence Integrity** profile tells reviewers what evidence is strong enough for the module artifact built around **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records**.

17.3.3.1 OSINT Techniques and Tools guide source spine: inherited keys and local citation roles Primary guide citations: [251, 2026]; [252, 2026]; [269, 2026]; [276, 2026]; [277, 2026]; [284, 2026]; [288, 2026]; [289, 2026]; [293, 2026]; [050, 2026]; [051, 2026]; [052, 2026]; [053, 2026]; [054, 2026]; [055, 2026]; [056, 2026].

17.3.3.2 OSINT Techniques and Tools verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [251, 2026]; [252, 2026].

Tier	What counts	How it is used
Source guide	[251, 2026]; [252, 2026]; [269, 2026]; [276, 2026]; [277, 2026]; [284, 2026]; [288, 2026]; [289, 2026]; [293, 2026]; [050, 2026]; [051, 2026]; [052, 2026]; [053, 2026]; [054, 2026]; [055, 2026]; [056, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 10's source-canon section, directly verified anchors for the **Open-Source and Geospatial Intelligence Integrity** lane include [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]; [Agency, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records** and [251, 2026]; [252, 2026], but only directly verified source URLs are encoded as citations.

17.3.3.3 OSINT Techniques and Tools intelligence practice lens: evidence artifact and safety check Practice lens: **Requirements-to-Evidence Lens** for **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records**. [251, 2026]; [252, 2026].

Planning question: What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit?

Evidence artifact: requirements matrix with source descriptors, caveats, and collection limits.

Validation rule: show priority, authority, minimization, corroboration, and source quality before any claim is reused. Applied to **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records**.

Handoff contract: deliver metadata-rich evidence packets, not unscoped data piles or implicit targeting requests.

Safety check: exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure.

17.3.3.4 OSINT Techniques and Tools runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 17; [251, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	10.99	10.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind OSINT Techniques and Tools to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Bounded autonomy, procurement, incident-response, and assurance studio	10.101	10.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for OSINT Techniques and Tools	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Model-card, recoverability, retention, and learner-support evidence package	10.102	10.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for OSINT Techniques and Tools	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Search-exposure provenance review using instructor-provided records	10.1	10.1 source title transformed into safe curriculum treatment; original: Search Engine Tradecraft: Google Dorking, Yandex, Bing, Shodan	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Social-source provenance and minimization review using toy records	10.2	10.2 source title transformed into safe curriculum treatment; original: Social Media OSINT: Scraping, Graph Analysis, Identity Verification	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Graph-analysis provenance review using instructor-provided records	10.3	10.3 source title transformed into safe curriculum treatment; original: Maltego: Graph-Based OSINT Investigation	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Custom-source integration governance review using toy records	10.4	10.4 source title transformed into safe curriculum treatment; original: Recon-ng: Python-Based Reconnaissance Framework	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Automated-source aggregation governance review using toy records	10.5	10.5 source title transformed into safe curriculum treatment; original: SpiderFoot: Automated OSINT Collection	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Identity-data minimization review using instructor-provided records	10.6	10.6 source title transformed into safe curriculum treatment; original: FOCA, TheHarvester, Sherlock: Targeted Investigation Tools	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
OSINT Framework (osintframework.com): Module Taxonomy	10.7	10.7 OSINT Framework (osint-framework.com): Module Taxonomy	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Offline OSINT Environments: VM Architecture and Isolation	10.8	10.8 Offline OSINT Environments: VM Architecture and Isolation	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
IntelTechniques OSINT 11th Edition Methods and Workflows	10.9	10.9 IntelTechniques OSINT 11th Edition Methods and Workflows	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

17.3.3.5 OSINT Techniques and Tools reusable subsection contract: topic rows, artifacts, and safety duties **Evidence anchor.** Section 17; [251, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Search-exposure provenance review using instructor-provided records	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Social-source provenance and minimization review using toy records	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Graph-analysis provenance review using instructor-provided records	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Custom-source integration governance review using toy records	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Automated-source aggregation governance review using toy records	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Identity-data minimization review using instructor-provided records	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

Lesson topic	Practice lens	Evidence artifact	Safety check
OSINT Framework (osintframework.com): Module Taxonomy	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Offline OSINT Environments: VM Architecture and Isolation	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
IntelTechniques OSINT 11th Edition Methods and Workflows	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

17.3.3.6 OSINT Techniques and Tools annotated source ledger: real titles and local contribution Each source cited by this **Open-Source and Geospatial Intelligence Integrity** module is paired below with its real title and a one-line note on what it contributes to **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records**.

Source	Cited work	What it contributes	Status
[251, 2026]	European Data Governance Act	The European Commission page explaining the Data Governance Act, an EU regulation that became applicable in September 2023 to build trust in data sharing and ease reuse of data. It outlines four mechanisms: facilitating reuse of protected public-sector data, establishing trusted data intermediaries, enabling voluntary data sharing by citizens and businesses, and removing barriers to cross-sector and cross-border data use.	verified source-guide
[252, 2026]	Data Act Explained	An official European Commission explainer on the EU Data Act, which became applicable on 12 September 2025.	verified source-guide
[269, 2026]	Data on the Web Best Practices	A W3C Recommendation, "Data on the Web Best Practices," published January 31, 2017 by the Data on the Web Best Practices Working Group. It offers 35 best practices for publishing and consuming data on the Web, covering metadata, licensing and provenance, data quality, dataset versioning, persistent URIs, machine-readable formats, vocabulary reuse, access methods, preservation, and feedback.	verified source-guide
[276, 2026]	What is a Data Protection Impact Assessment and When Is This Mandatory?	A European Data Protection Board FAQ page, part of its data protection guide for small businesses, explaining Data Protection Impact Assessments (DPIAs) and when they are mandatory. It describes a DPIA as a written assessment of the impact of a planned processing operation, required when processing poses high risks to individuals' rights.	verified source-guide
[277, 2026]	Endorsed WP29 Guidelines	This is a European Data Protection Board webpage listing guidelines and documents originating from the Article 29 Working Party that the EDPB endorsed at its first plenary meeting. The catalogued materials relate to the GDPR and cover topics such as consent and transparency, data breach notification, automated decision-making and profiling, data protection impact assessments, data protection officers, and binding corporate rules.	verified source-guide

Source	Cited work	What it contributes	Status
[284, 2026]	Verifiable Credential Data Integrity 1.0	The W3C Recommendation for Verifiable Credential Data Integrity 1.0, published May 2025, defining mechanisms for ensuring the authenticity and integrity of verifiable credentials using cryptographic proofs. It specifies a process of data transformation, hashing, and proof generation, and a corresponding verification procedure, along with a proof data model containing properties such as type, verification method, purpose, and proof value.	verified source-guide
[288, 2026]	Algorithmic Transparency Recording Standard Hub	A GOV.UK collection page serving as the hub for the UK Algorithmic Transparency Recording Standard (ATRS), maintained by the Government Digital Service. It provides a standardized template for documenting public-sector use of algorithmic tools, completion guidance, policy on scope and compliance, and a searchable repository of published transparency records.	verified source-guide
[289, 2026]	Guidance for Organisations Using the Algorithmic Transparency Recording Standard	This is a GOV.UK guidance page published by the Government Digital Service that instructs public sector organizations on completing the Algorithmic Transparency Recording Standard (ATRS) template and publishing their records to the GOV.UK repository. It applies both to central government bodies required to publish under mandatory policy and to other public sector bodies doing so voluntarily.	verified source-guide
[293, 2026]	Inventory of NARA Artificial Intelligence (AI) Use Cases	The National Archives and Records Administration (NARA) official inventory of its artificial intelligence use cases, documenting 14 projects across deployed, pilot, and planned stages. Deployed efforts include workplace productivity tools, automated tagging for museum experiences, and historical record retrieval, while pilots cover PII detection and redaction, semantic search, and metadata generation, and planned work targets FOIA processing and public search.	verified source-guide
[050, 2026]	[Thoughts on Bazzell's New Book? Open Source Intelligence	Mike wrote he wants to make the OSINT investigator more self reliant, able to do his job without.	original source-guide
[051, 2026]	Cited source (see bibliography)	See bibliography for scope.	original source-guide
[052, 2026]	What is Open Source Intelligence & Top 10 Tools - Lampyre	This article defines open source intelligence as the practice of gathering information from publicly available data for security, business, and investigative purposes, drawing on websites, social media, government records, and public databases.	verified source-guide
[053, 2026]	A Guide to Choosing the Right Tool for Your Needs	See bibliography for scope.	verified practitioner context; secondary evidence only
[054, 2026]	What are your preferred OSINT tools? : r/hacking	Recommended OSINT tools and their benefits. Top open source intelligence websites.	original source-guide
[055, 2026]	IntelTechniques Books	OSINT Techniques. Resources for Uncovering Online Information - 11th Edition (2024).	original source-guide
[056, 2026]	IntelTechniques - OSINT 11 2025.04.02 .pdf - elhacker.INFO	All tutorials in this book were confirmed accurate as of November 1, 2024.	original source-guide

Where this sits. This module's overview is Section 17; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates

that govern this module.

17.3.4 OSINT Techniques and Tools governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 17; [251, 2026].

17.3.5 OSINT Techniques and Tools analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 10's governance-boundary section, directly verified anchors for the **Open-Source and Geospatial Intelligence Integrity** lane include [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]; [Agency, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Research lane: **Open-Source and Geospatial Intelligence Integrity** for **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records**. [251, 2026]; [252, 2026].
Curriculum topic spine: Search-exposure provenance review using instructor-provided records, **Social-source provenance and minimization review using toy records**, **Graph-analysis provenance review using instructor-provided records**. **Verified anchor cluster:** [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]; [Agency, 2026b]; [for Standardization, 2013]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015].
Conceptual depth: public-source discovery converted into accountable intelligence through provenance, corroboration, minimization, and relevance tests.
Method stack: source triage, provenance capture, corroboration matrix, recency audit, geospatial context review, and confidence calibration.
Composability contract: collection notes, source metadata, transformations, caveats, and analytic judgments remain separately exportable.
Known failure modes: privacy drift, stale data, context collapse, platform bias, over-collection, and mistaking availability for reliability.
Defensive boundary: OSINT work uses lawful public, owned-lab, or explicitly approved sources and avoids doxxing, harassment, live tracking, or operational targeting. Applied to **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records**.

Anchor	Why it matters here
[of the Director of National Intelligence and Agency, 2024]	Official IC OSINT strategy for professionalizing OSINT, integrated collection management, open-source sharing, innovation, and tradecraft. Checked as of 2026-05-21; role: curriculum_anchor.
[of State, 2024]	Official strategy source for lawful OSINT governance, discovery, validation, and dissemination. Checked as of 2026-05-21; role: curriculum_anchor.
[Agency, 2026c]	Official NGA strategy anchor for GEOINT readiness, warning, partnership resilience, resource stewardship, and AI integration. Checked as of 2026-05-21; role: curriculum_anchor.
[Agency, 2026b]	Official NGA source on GEOINT AI, data quality, model performance, interoperability, analyst interaction, and standards leadership. Checked as of 2026-05-21; role: curriculum_anchor.
[for Standardization, 2013]	International geospatial data-quality standard for completeness, logical consistency, positional accuracy, temporal quality, and usability framing. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026d]	Official sourcing directive for traceability, citations, source descriptors, and source summaries. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2015]	Official ODNI analytic tradecraft standards directive. Checked as of 2026-05-21; role: source_quality_anchor.

17.3.5.1 OSINT Techniques and Tools evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **Open-Source and Geospatial Intelligence Integrity** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [251, 2026]; [252, 2026].

17.3.6 OSINT Techniques and Tools agentic boundary: assist, approve, block, and record

Evidence anchor. Section 17; [251, 2026].
AGEINT translation is bounded by the **Open-Source and Geospatial Intelligence Integrity** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records**.

17.3.6.1 OSINT Techniques and Tools permitted defensive utility: curriculum uses and safe outputs

Evidence anchor. Section 17; [251, 2026].
The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records**.

17.3.6.2 OSINT Techniques and Tools excluded operational boundary: blocked actions and stop rules

Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [251, 2026]; [252, 2026] and **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

17.3.7 OSINT Techniques and Tools governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 17; [251, 2026].
Governance is practiced as a gate on the **Open-Source and Geospatial Intelligence Integrity** lane. Learners use the **Requirements-to-Evidence Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records**.

17.3.7.1 OSINT Techniques and Tools governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [251, 2026]; [252, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Open-Source and Geospatial Intelligence Integrity** failure modes and the **Requirements-to-Evidence Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

17.3.7.2 OSINT Techniques and Tools evidence package handoff: appendices, records, and reuse

Evidence anchor. Section 17; [251, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Requirements-to-Evidence Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records**.

17.3.7.3 OSINT Techniques and Tools current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records**. [251, 2026]; [252, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_ic_osint_strategy` for **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records**?	The INT of First Resort: The IC OSINT Strategy 2024-2026; lane `osint_geoint`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official IC OSINT strategy for professionalizing OSINT, integrated collection management, open-source sharing, innovation, and tradecraft.
What does the module inherit from `official_state_osint_strategy` for **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records**?	Open Source Intelligence Strategy; lane `osint_geoint`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official strategy source for lawful OSINT governance, discovery, validation, and dissemination.
What does the module inherit from `official_nga_strategy` for **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records**?	NGA Strategy; lane `osint_geoint`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official NGA strategy anchor for GEOINT readiness, warning, partnership resilience, resource stewardship, and AI integration.
What does the module inherit from `official_nga_geoint_ai` for **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records**?	GEOINT Artificial Intelligence; lane `osint_geoint`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official NGA source on GEOINT AI, data quality, model performance, interoperability, analyst interaction, and standards leadership.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 17; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

17.3.8 OSINT Techniques and Tools assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 17; [251, 2026].

17.3.9 OSINT Techniques and Tools assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 17; [251, 2026].

17.3.9.1 OSINT Techniques and Tools capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records** and [251, 2026]; [252, 2026].

17.3.9.2 OSINT Techniques and Tools instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records** and [251, 2026]; [252, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

17.3.9.3 OSINT Techniques and Tools assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Search-exposure provenance review using instructor-provided records	Completed **requirements matrix with source descriptors, caveats, and collection limits** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Social-source provenance and minimization review using toy records	Completed **requirements matrix with source descriptors, caveats, and collection limits** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Graph-analysis provenance review using instructor-provided records	Completed **requirements matrix with source descriptors, caveats, and collection limits** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

17.3.10 OSINT Techniques and Tools refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [251, 2026]; [252, 2026] and **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records**.

17.3.10.1 OSINT Techniques and Tools refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records**. The local signals begin with [251, 2026]; [252, 2026].

17.3.10.2 OSINT Techniques and Tools claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records**, and the source spine for these checks begins with [251, 2026]; [252, 2026].

17.3.11 OSINT Techniques and Tools reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [251, 2026]; [252, 2026].

Triangulation anchors. In module 10's review-checklist section, directly verified anchors for the **Open-Source and Geospatial Intelligence Integrity** lane include [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]; [Agency, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records**. [251, 2026]; [252, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

17.3.12 OSINT Techniques and Tools learning-path links: module map, overview, and curriculum atlas

Use the cross-links below to place **Search-exposure provenance review using instructor-provided records; Social-source provenance and minimization review using toy records** in the wider unit: the orientation sets the frame, the parent unit supplies the shared safety posture, and the neighbouring modules show what evidence enters and leaves. Lead sources: [251, 2026]; [252, 2026].

Section 2, Section 15, Section 16, Section 18

18 GEOINT and Imagery Intelligence

18.0.1 GEOINT and Imagery Intelligence figures and course links: visual evidence, source flow, and navigation

The module uses Figure 49, Figure 50, Figure 51, and Figure 45 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 15, Section 17, Section 19.
This module teaches the **Open-Source and Geospatial Intelligence Integrity** lane through a bounded, source-backed coursebook chapter. [253, 2026]; [255, 2026].

18.1 Open-Source and Geospatial Intelligence Integrity frame for GEOINT and Imagery Intelligence: source context, topic focus, and reader task

Evidence anchor. Section 18; [253, 2026].

18.1.1 GEOINT and Imagery Intelligence orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 18; [253, 2026].

18.1.2 GEOINT and Imagery Intelligence conceptual primer: source context, core model, and reader task

This chapter teaches OSINT and GEOINT as public-source reasoning disciplines: availability does not equal reliability, relevance, legality, or ethical reuse. The chapter uses **Requirements-to-Evidence Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**.
The central distinction is to separate discovery from collection expansion, and map or media interpretation from targeting. Core topics include **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples; Imagery collection-platform literacy: resolution and revisit tradeoffs**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [253, 2026]; [255, 2026].
Learners move from vocabulary and the **Requirements-to-Evidence Lens** distinction through topic lessons on **Imagery quality literacy: resolution, temporal fit, and uncertainty** with evidence and misconception checks, then assemble a **requirements matrix with source descriptors, caveats, and collection limits** with safety and rights gates.

18.1.3 GEOINT and Imagery Intelligence learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 18; [253, 2026].

- Connect **Imagery quality literacy: resolution, temporal fit, and uncertainty and GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples** to **Open-Source and Geospatial Intelligence Integrity** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **requirements matrix with source descriptors, caveats, and collection limits** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate discovery from collection expansion, and map or media interpretation from targeting; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as privacy drift, stale data, context collapse, platform bias, over-collection, and mistaking availability for reliability, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: OSINT work uses lawful public, owned-lab, or explicitly approved sources and avoids doxxing, harassment, live tracking, or operational targeting.

18.1.4 GEOINT and Imagery Intelligence core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 18; [253, 2026].

Term	Working definition
Provenance	the origin, chain, and transformation history of a source
Corroboration	the comparison of independent sources before reuse
Recency	the time relationship between source creation, discovery, and claim
Geospatial quality	accuracy, completeness, temporal fitness, and usability of location data
Minimization	limiting retained information to what the accountable question requires
Imagery quality literacy: resolution, temporal…	Key terms: Imagery, quality, literacy.
GEOINT data-quality audit using provided…	Key terms: GEOINT, data, quality.

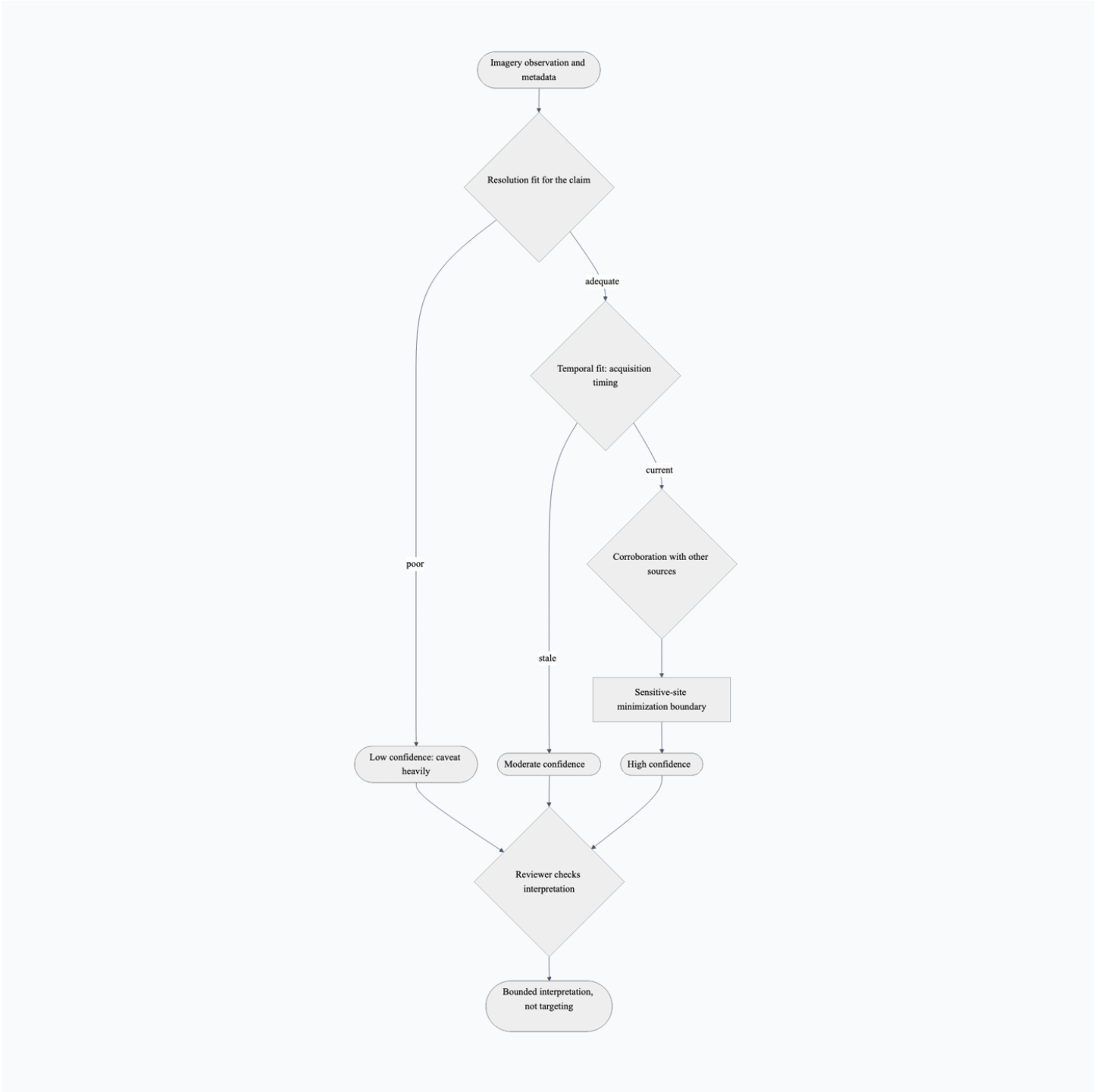


Figure 49: This diagram presents a confidence ladder that ties an imagery interpretation's defensibility to resolution fit, temporal fit, corroboration, and an explicit sensitive-site boundary that separates map reading from targeting or attribution. In the open source intelligence osint / geoint and imagery intelligence section, it lets readers compare Imagery observation and metadata, Sensitive-site minimization boundary, Low confidence: caveat heavily, and Moderate confidence so the visual functions as a traceable course aid rather than an unscoped assertion.

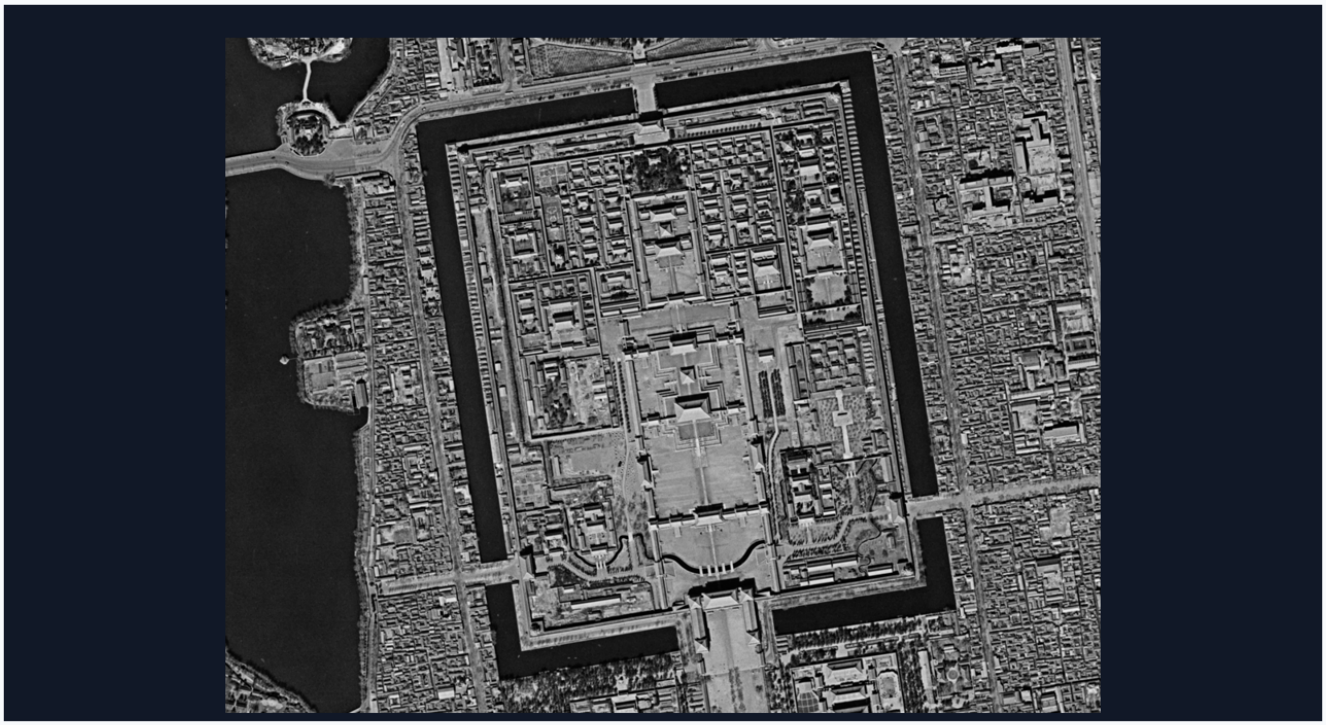


Figure 50: Public-domain USGS EROS declassified imagery of the Forbidden City as a local historical image for GEOINT source-provenance discussion. Its reader value is to make U.S. Geological Survey provenance, 1966 approx. collection context, public-domain status, and analytic reuse boundary visible at a glance, with the open source intelligence osint / geoint and imagery intelligence section as the source section and defensive review as the boundary.

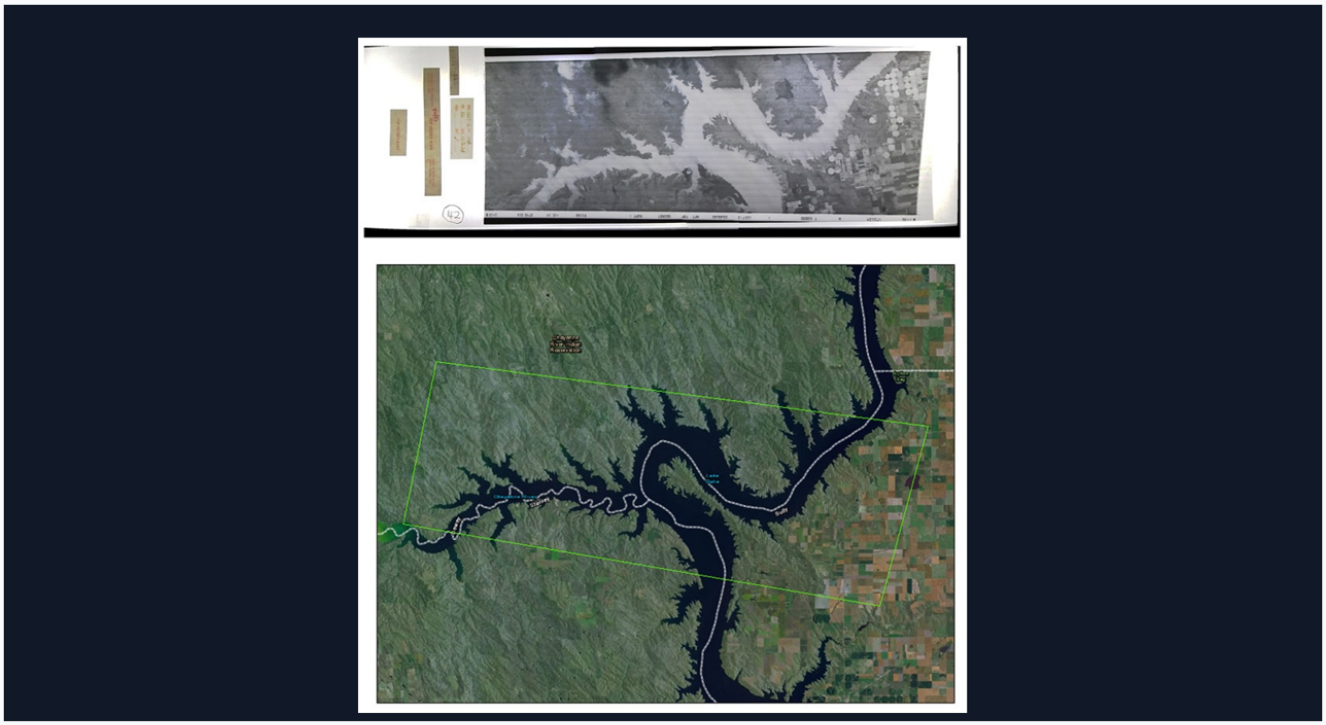


Figure 51: Public-domain USGS EROS KH-9 image used as a historical example of declassified remote-sensing material with explicit provenance. It is anchored to the open source intelligence osint / geoint and imagery intelligence section; use it to inspect U.S. Geological Survey provenance, 1982-07-22 collection context, public-domain status, and analytic reuse boundary while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

18.2 Requirements-to-Evidence Lens path for GEOINT and Imagery Intelligence: lesson cluster, safe artifact, and review

Evidence anchor. Section 18; [253, 2026].

18.2.1 GEOINT and Imagery Intelligence practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 18; [253, 2026].

18.2.2 GEOINT and Imagery Intelligence topic lessons: source-backed concepts and transfer tasks

This module builds OSINT and GEOINT as public-source reasoning disciplines: availability does not equal reliability, relevance, legality, or ethical reuse. The sequence opens with **Imagery quality literacy: resolution, temporal fit, and uncertainty**, **GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**, **Imagery collection-platform literacy: resolution and revisit tradeoffs** and applies the **Requirements-to-Evidence Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 45; module overview Section 18; curriculum atlas Section 2.

Triangulation anchors. In module 11's topic-lessons section, directly verified anchors for the **Open-Source and Geospatial Intelligence Integrity** lane include [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]; [Agency, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

18.2.2.1 Lesson 1: Imagery quality literacy: resolution, temporal fit, and uncertainty

Concept. Imagery quality literacy: resolution, temporal fit, and uncertainty treats location evidence as a quality and uncertainty problem, separating map interpretation from targeting or attribution.

Why it matters. Analysts use **Imagery quality literacy** to separate discovery from collection expansion, and map or media interpretation from targeting. A defensible treatment names the judgment it enables for source-quality review and non-sensitive geospatial interpretation review, the proof limit that privacy drift would otherwise hide, and the reviewer accountable for challenge.

Source support. Imagery quality literacy: resolution, temporal fit, and uncertainty rests on [057, 2026]. Its anchor reference records: MCRP 2-10B.4 in the source guide links to the Marines GEOINT manual, not a reconnaissance manual. Use it for pinning down the scope of **Imagery quality literacy: resolution, temporal fit, and uncertainty**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. Ground **Imagery quality literacy** in the evidence the row cites. [057, 2026] MCRP 2-10B.4 in the source guide links to the Marines GEOINT manual, not a reconnaissance manual. The linked PDF is 'Geospatial Intelligence Support to Operations'; verify the intended citation before reuse. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Imagery quality literacy**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this source-quality review and non-sensitive geospatial interpretation topic. The artifact must list the imagery descriptor, the bounded claim about **Imagery quality literacy**, the resolution caveat, the uncertainty note, the sensitive-site boundary, and the reviewer who checks the interpretation. Shape **Imagery quality literacy** work as an **OSINT provenance and minimization matrix** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Imagery quality literacy**: that a visible feature is enough for a confident geospatial claim.

Transfer task. Transfer **Imagery quality literacy** from this module to a second motif by preserving source-quality review and non-sensitive geospatial interpretation, replacing action with audit, and naming the blocked use.

18.2.2.2 Lesson 2: GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples

Concept. GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples treats metadata as a distinct evidence class with its own minimization, correlation limits, and legal review requirements.

Why it matters. Analysts use **GEOINT data-quality audit** to separate discovery from collection expansion, and map or media interpretation from targeting. A defensible treatment names the judgment it enables for source-quality review and non-sensitive geospatial interpretation review, the proof limit that privacy drift would otherwise hide, and the reviewer accountable for challenge.

Source support. GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples rests on [058, 2026]. The closest source to this row notes: First developed in 2014 and revised with community input, it defines the competencies, standards, and learning objectives needed to succeed in the geospatial intelligence discipline. Use it for pinning down the scope of **GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. For **GEOINT data-quality audit**, reason from the sources cited in this row. [058, 2026] The GEOINT Essential Body of Knowledge (Version 2.0, 2019), published by the United States Geospatial Intelligence Foundation (USGIF). First developed in 2014 and revised with community input, it defines the competencies, standards, and learning objectives needed to succeed in the geospatial intelligence discipline. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **GEOINT data-quality audit**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this source-quality review and non-sensitive geospatial interpretation topic. The artifact must list the imagery descriptor, the bounded claim about **GEOINT data-quality audit using provided**, the resolution caveat, the uncertainty note, the sensitive-site boundary, and the reviewer who checks the interpretation. Shape **GEOINT data-quality audit** work as an **OSINT provenance and minimization matrix** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **GEOINT data-quality audit**: that a visible feature is enough for a confident geospatial claim.

Transfer task. Transfer **GEOINT data-quality audit** from this module to a second motif by preserving source-quality review and non-sensitive geospatial interpretation, replacing action with audit, and naming the blocked use.

18.2.2.3 Lesson 3: Imagery collection-platform literacy: resolution and revisit tradeoffs

Concept. Imagery collection-platform literacy: resolution and revisit tradeoffs treats location evidence as a quality and uncertainty problem, separating map interpretation from targeting or attribution.

Why it matters. Imagery collection-platform literacy connects classroom vocabulary to Open-Source and Geospatial Intelligence Integrity practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Imagery collection-platform literacy: resolution and revisit tradeoffs rests on [059, 2026]. The most specific cited work observes: It curates open-source resources organized into categories including satellite imagery, mapping, infrastructure and transport tracking, weather and environmental monitoring, shadow and sun-position tools for time-of-day analysis, crisis and conflict mapping, image forensics, and geocoding utilities. Use it for the working definition that **Imagery collection-platform literacy: resolution and revisit tradeoffs** can defend, where that

scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. For **Imagery collection-platform literacy**, work from the cited evidence behind this row. [059, 2026] A GitHub repository describing itself as a reference toolkit for geolocation and chronolocation in digital investigations. It curates open-source resources organized into categories including satellite imagery, mapping, infrastructure and transport tracking, weather and environmental monitoring, shadow and sun-position tools for time-of-day analysis, crisis and conflict mapping, image forensics, and geocoding utilities. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Imagery collection-platform literacy**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this source-quality review and non-sensitive geospatial interpretation topic. The artifact must list the imagery descriptor, the bounded claim about **Imagery collection-platform literacy**, the resolution caveat, the uncertainty note, the sensitive-site boundary, and the reviewer who checks the interpretation. Shape **Imagery collection-platform literacy** work as an **OSINT provenance and minimization matrix** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Imagery collection-platform literacy**: that a visible feature is enough for a confident geospatial claim.

Transfer task. Transfer **Imagery collection-platform literacy** from this module to a second motif by preserving source-quality review and non-sensitive geospatial interpretation, replacing action with audit, and naming the blocked use.

18.2.2.4 Lesson 4: Claim-ledger memory exercise that tracks evidence changes rather than people

Concept. Claim-ledger memory exercise that tracks evidence changes rather than people treats location evidence as a quality and uncertainty problem, separating map interpretation from targeting or attribution.

Why it matters. Analysts use **Claim-ledger memory exercise that tracks evidence changes rather than people** to separate discovery from collection expansion, and map or media interpretation from targeting. A defensible treatment names the judgment it enables for source-quality review and non-sensitive geospatial interpretation review, the proof limit that privacy drift would otherwise hide, and the reviewer accountable for challenge.

Source support. Claim-ledger memory exercise that tracks evidence changes rather than people rests on [302, 2026] and [297, 2026]. The lead source's own note reads: The official "About Us" page of the National Geospatial-Intelligence Agency (NGA), a U.S. Use them for the working definition that **Claim-ledger memory exercise that tracks evidence changes rather than people** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. For **Claim-ledger memory exercise that tracks evidence changes rather than people**, reason from the sources cited in this row. [302, 2026] The official "About Us" page of the National Geospatial-Intelligence Agency (NGA), a U.S. Department of Defense and intelligence community organization. It describes NGA's mission of delivering geospatial intelligence, or GEOINT, to support military operations, policymakers, and first responders, spanning imagery analysis, mapping, geodesy, and navigation safety. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Claim-ledger memory exercise that tracks evidence changes rather than people**, build a claim-ledger memory card with source descriptor, source-change event, retention rule, contamination check, and reviewer disposition; it must not track real people, assets, or behavioral patterns. Shape this subject work as an **OSINT provenance and minimization matrix** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Claim-ledger memory exercise that tracks evidence changes rather than people**: that a visible feature is enough for a confident geospatial claim.

Transfer task. Reuse the **Claim-ledger memory exercise that tracks evidence changes rather than people** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

18.2.2.5 Lesson 5: GEOINT in Counterinsurgency and Strike: GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples

Concept. GEOINT in Counterinsurgency and Strike: GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples treats metadata as a distinct evidence class with its own minimization, correlation limits, and legal review requirements.

Why it matters. Without explicit treatment of **GEOINT in Counterinsurgency and Strike**, privacy drift undermines source-quality review and non-sensitive geospatial interpretation review; the lesson builds the habit to separate discovery from collection expansion, and map or media interpretation from targeting.

Source support. GEOINT in Counterinsurgency and Strike: GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples rests on [302, 2026] and [297, 2026]. The closest source to this row notes: It describes NGA's mission of delivering geospatial intelligence, or GEOINT, to support military operations, policymakers, and first responders, spanning imagery analysis, mapping, geodesy, and navigation safety. Use them for the working definition that **GEOINT in Counterinsurgency and Strike: GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. Read **GEOINT in Counterinsurgency and Strike** against the works cited for this row. [302, 2026] The official "About Us" page of the National Geospatial-Intelligence Agency (NGA), a U.S. Department of Defense and intelligence community organization. It describes NGA's mission of delivering geospatial intelligence, or GEOINT, to support military operations, policymakers, and first responders, spanning imagery analysis, mapping, geodesy, and navigation safety. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **GEOINT in Counterinsurgency and Strike**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this source-quality review and non-sensitive geospatial interpretation topic. The artifact must list the imagery descriptor, the bounded claim about **GEOINT in Counterinsurgency and Strike**, the resolution caveat, the uncertainty note, the sensitive-site boundary, and the reviewer who checks the interpretation. Shape **GEOINT in Counterinsurgency and Strike** work as an **OSINT provenance and minimization matrix** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **GEOINT in Counterinsurgency and Strike**: that a visible feature is enough for a confident geospatial claim.

Transfer task. Transfer **GEOINT in Counterinsurgency and Strike** from this module to a second motif by preserving source-quality review and non-sensitive geospatial interpretation, replacing action with audit, and naming the blocked use.

18.2.2.6 Lesson 6: DoD GEOINT Accreditation and Training: GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples

Concept. DoD GEOINT Accreditation and Training: GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples treats metadata as a distinct evidence class with its own minimization, correlation limits, and legal review requirements.

Why it matters. DoD GEOINT Accreditation and Training connects classroom vocabulary to Open-Source and Geospatial Intelligence Integrity practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. DoD GEOINT Accreditation and Training: GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples rests on [060, 2026]. Use it for fixing what **DoD GEOINT Accreditation and Training: GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. Ground **DoD GEOINT Accreditation and Training** in the evidence the row cites. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **DoD GEOINT Accreditation and Training**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this source-quality review and non-sensitive geospatial interpretation topic. The artifact must list the imagery descriptor, the bounded claim about **DoD GEOINT Accreditation and Training**, the resolution caveat, the uncertainty note, the sensitive-site boundary, and the reviewer who checks the interpretation. Shape **DoD GEOINT Accreditation and Training** work as an **OSINT provenance and minimization matrix** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **DoD GEOINT Accreditation and Training**: that a visible feature is enough for a confident geospatial claim.

Transfer task. Transfer **DoD GEOINT Accreditation and Training** from this module to a second motif by preserving source-quality review and non-sensitive geospatial interpretation, replacing action with audit, and naming the blocked use.

18.2.2.7 Lesson 7: MCRP 2-10B 4: GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples

Concept. MCRP 2-10B 4: GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples treats metadata as a distinct evidence class with its own minimization, correlation limits, and legal review requirements.

Why it matters. Without explicit treatment of **MCRP 2-10B 4: GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**, privacy drift undermines source-quality review and non-sensitive geospatial interpretation review; the lesson builds the habit to separate discovery from collection expansion, and map or media interpretation from targeting.

Source support. MCRP 2-10B 4: GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples rests on [057, 2026]. The most specific cited work observes: MCRP 2-10B.4 in the source guide links to the Marines GEOINT manual, not a reconnaissance manual. Use it for the working definition that **MCRP 2-10B 4: GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. Read **MCRP 2-10B 4: GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples** against the works cited for this row. [057, 2026] MCRP 2-10B.4 in the source guide links to the Marines GEOINT manual, not a reconnaissance manual. The linked PDF is 'Geospatial Intelligence Support to Operations'; verify the intended citation before reuse. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **MCRP 2-10B 4**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this source-quality review and non-sensitive geospatial interpretation topic. The artifact must list the imagery descriptor, the bounded claim about **MCRP 2-10B 4**, the resolution caveat, the uncertainty note, the sensitive-site boundary, and the reviewer who checks the interpretation. Shape **MCRP 2-10B 4: GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples** work as an **OSINT provenance and minimization matrix** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **MCRP 2-10B 4: GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**: that a visible feature is enough for a confident geospatial claim.

Transfer task. Reuse the **MCRP 2-10B 4: GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

18.2.2.8 Lesson 8: AI-Assisted Satellite Image Analysis: Imagery collection-platform literacy: resolution and revisit tradeoffs

Concept. AI-Assisted Satellite Image Analysis: Imagery collection-platform literacy: resolution and revisit tradeoffs treats location evidence as a quality and uncertainty problem, separating map interpretation from targeting or attribution.

Why it matters. AI-Assisted Satellite Image Analysis matters in the **Open-Source and Geospatial Intelligence Integrity** lane because source-quality review and non-sensitive geospatial interpretation evidence must stay separate from judgment; privacy drift is a common failure.

Source support. AI-Assisted Satellite Image Analysis: Imagery collection-platform literacy: resolution and revisit tradeoffs rests on [302, 2026] and [297, 2026]. Its anchor reference records: The official "About Us" page of the National Geospatial-Intelligence Agency (NGA), a U.S. Use them for the working definition that **AI-Assisted Satellite Image Analysis: Imagery collection-platform literacy: resolution and revisit tradeoffs** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. Read **AI-Assisted Satellite Image Analysis** against the works cited for this row. [302, 2026] The official "About Us" page of the National Geospatial-Intelligence Agency (NGA), a U.S. Department of Defense and intelligence community organization. It describes NGA's mission of delivering geospatial intelligence, or GEOINT, to support military operations, policymakers, and first responders, spanning imagery analysis, mapping, geodesy, and navigation safety. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **AI-Assisted Satellite Image Analysis**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this source-quality review and non-sensitive geospatial interpretation topic. The artifact must list the imagery descriptor, the bounded claim about **AI-Assisted Satellite Image Analysis**, the resolution caveat, the uncertainty note, the sensitive-site boundary, and the reviewer who checks the interpretation. Shape **AI-Assisted Satellite Image Analysis** work as an **OSINT provenance and minimization matrix** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **AI-Assisted Satellite Image Analysis**: that a visible feature is enough for a confident geospatial claim.

Transfer task. Apply this module's safe boundary for **AI-Assisted Satellite Image Analysis** to another artifact while keeping source-quality review and non-sensitive geospatial interpretation and reviewer ownership explicit.

18.2.2.9 Lesson 9: Open-Source Geospatial Intelligence Library: GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples

Concept. Open-Source Geospatial Intelligence Library: GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples treats metadata as a distinct evidence class with its own minimization, correlation limits, and legal review requirements.

Why it matters. Without explicit treatment of **Open-Source Geospatial Intelligence Library**, privacy drift undermines source-quality review and non-sensitive geospatial interpretation review; the lesson builds the habit to separate discovery from collection expansion, and map or media interpretation from targeting.

Source support. Open-Source Geospatial Intelligence Library: GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples rests on [059, 2026]. The most specific cited work observes: It curates open-source resources organized

into categories including satellite imagery, mapping, infrastructure and transport tracking, weather and environmental monitoring, shadow and sun-position tools for time-of-day analysis, crisis and conflict mapping, image forensics, and geocoding utilities. Use it for the claim that **Open-Source Geospatial Intelligence Library: GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. Read **Open-Source Geospatial Intelligence Library** against the works cited for this row. [059, 2026] A GitHub repository describing itself as a reference toolkit for geolocation and chronolocation in digital investigations. It curates open-source resources organized into categories including satellite imagery, mapping, infrastructure and transport tracking, weather and environmental monitoring, shadow and sun-position tools for time-of-day analysis, crisis and conflict mapping, image forensics, and geocoding utilities. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Open-Source Geospatial Intelligence Library**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this source-quality review and non-sensitive geospatial interpretation topic. The artifact must list the imagery descriptor, the bounded claim about **Open-Source Geospatial Intelligence Library**, the resolution caveat, the uncertainty note, the sensitive-site boundary, and the reviewer who checks the interpretation. Shape **Open-Source Geospatial Intelligence Library** work as an **OSINT provenance and minimization matrix** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Open-Source Geospatial Intelligence Library**: that a visible feature is enough for a confident geospatial claim.

Transfer task. Apply this module's safe boundary for **Open-Source Geospatial Intelligence Library** to another artifact while keeping source-quality review and non-sensitive geospatial interpretation and reviewer ownership explicit.

18.2.3 GEOINT and Imagery Intelligence worked safe example: synthetic inputs, evidence, and review

Worked example: a synthetic public-resilience team checks whether open data supports a non-sensitive evacuation-route map. [253, 2026]; [255, 2026].

Triangulation anchors. In module 11's worked-example section, directly verified anchors for the **Open-Source and Geospatial Intelligence Integrity** lane include [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]; [Agency, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **open-source intelligence governance**. Learners use a **OSINT provenance and minimization matrix** and keep this boundary visible: No exposed-service lookup, credentialed access, identity exposure, doxxing, or live collection expansion.

Frame. The classroom question centers on **Imagery quality literacy: resolution, temporal fit, and uncertainty**. Excluded actions stay explicit, and the **Requirements-to-Evidence Lens** planning question is: What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit?

Inputs. For the **Imagery quality literacy: resolution, temporal fit, and uncertainty** scenario, use public road data, public weather notices, synthetic change examples, and instructor-provided metadata. The Requirements-to-Evidence Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Imagery quality literacy: resolution, temporal fit, and uncertainty**, students record provenance, test recency, compare independent sources, mark uncertainty, and remove unnecessary identity data. Pause whenever an inference about Imagery quality literacy: resolution, temporal fit, and uncertainty appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Imagery quality literacy: resolution, temporal fit, and uncertainty** classroom scenario; unit artifact = OSINT provenance and minimization matrix; evidence = allowed inputs; method = source-quality review and non-sensitive geospatial interpretation; output = a source-quality matrix and annotated map note with caveats and no tracking or targeting content; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Imagery quality literacy: resolution, temporal fit, and uncertainty** as "Requirements-to-Evidence Lens confirms it" is not enough. The revision ties the claim to source-quality review and non-sensitive geospatial interpretation, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Imagery quality literacy: resolution, temporal fit, and uncertainty** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

18.2.4 GEOINT and Imagery Intelligence practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Requirements-to-Evidence Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**.

Triangulation anchors. In module 11's practice-sequence section, directly verified anchors for the **Open-Source and Geospatial Intelligence Integrity** lane include [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]; [Agency, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Imagery quality literacy: resolution, temporal fit, and uncertainty, GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples, Imagery collection-platform literacy: resolution and revisit tradeoffs; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Open-Source and Geospatial Intelligence Integrity** lane.
2. Frame	Answer the lens question: What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Imagery quality literacy: resolution, temporal fit, and uncertainty: requirements matrix with source descriptors, caveats, and collection limits.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.

Move	Learner action	Output	Check
3a. Unit artifact	Add the OSINT provenance and minimization matrix fields for Imagery quality literacy: resolution, temporal fit, and uncertainty.	Unit profile note.	Evidence artifacts include provenance chain, terms-of-use note.
4. Challenge	Test the misconception that a visible feature is enough for a confident geospatial claim.	Failure-mode note.	The artifact applies the key distinction: separate discovery from collection expansion, and map or media interpretation from targeting.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

18.2.4.1 GEOINT and Imagery Intelligence instructor notes: source reasoning, review points, and studio focus Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**. [253, 2026]; [255, 2026].

18.2.4.2 GEOINT and Imagery Intelligence extension exercise: peer validation and refresh trigger review **Evidence anchor.** Section 18; [253, 2026].
Have learners swap artifacts and apply the **Requirements-to-Evidence Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**.

18.2.5 GEOINT and Imagery Intelligence knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 18; [253, 2026].

1. Explain how **Imagery quality literacy: resolution, temporal fit, and uncertainty** is defined here; name the source descriptor that supports the definition.
2. Contrast **Imagery quality literacy: resolution, temporal fit, and uncertainty** with **GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples** using the **Requirements-to-Evidence Lens** artifact fields.
3. Identify one failure mode from the **Open-Source and Geospatial Intelligence Integrity** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which source is available but not reliable enough for the claim?
5. Correct this misconception: that a visible feature is enough for a confident geospatial claim.

18.2.5.1 GEOINT and Imagery Intelligence answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Imagery quality literacy: resolution, temporal fit, and uncertainty** without source evidence, uncertainty, or a safe transfer task.

18.3 GEOINT and Imagery Intelligence assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 18; [253, 2026].

18.3.1 GEOINT and Imagery Intelligence evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 18; [253, 2026].

18.3.2 GEOINT and Imagery Intelligence transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 18; [253, 2026].

18.3.2.1 GEOINT and Imagery Intelligence lineage and source tradition: profile, concepts, and first anchors This sits in the **Open-Source and Geospatial Intelligence Integrity** lineage: public-source discovery converted into accountable intelligence through provenance, corroboration, minimization, and relevance tests. [253, 2026]; [255, 2026].

18.3.2.2 GEOINT and Imagery Intelligence working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 18; [253, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**, with provenance and reviewability throughout.

18.3.2.3 GEOINT and Imagery Intelligence knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [253, 2026]; [255, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

18.3.2.4 GEOINT and Imagery Intelligence transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 18; [253, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**.
- **Evidence contract:** keep the **Open-Source and Geospatial Intelligence Integrity** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

18.3.2.5 GEOINT and Imagery Intelligence profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 18; [253, 2026].

The matched profile emphasizes public-source discovery converted into accountable intelligence through provenance, corroboration, minimization, and relevance tests. The method stack is source triage, provenance capture, corroboration matrix, recency audit, geospatial context review, and confidence calibration; the local topic cluster is **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**.

18.3.3 GEOINT and Imagery Intelligence evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 18; [253, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Open-Source and Geospatial Intelligence Integrity** profile tells reviewers what evidence is strong enough for the module artifact built around **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**.

18.3.3.1 GEOINT and Imagery Intelligence guide source spine: inherited keys and local citation roles Primary guide citations: [253, 2026]; [255, 2026]; [270, 2026]; [278, 2026]; [279, 2026]; [283, 2026]; [290, 2026]; [291, 2026]; [294, 2026]; [057, 2026]; [058, 2026]; [059, 2026]; [060, 2026]; [301, 2026]; [298, 2026]; [302, 2026]; [297, 2026].

18.3.3.2 GEOINT and Imagery Intelligence verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [253, 2026]; [255, 2026].

Tier	What counts	How it is used
Source guide	[253, 2026]; [255, 2026]; [270, 2026]; [278, 2026]; [279, 2026]; [283, 2026]; [290, 2026]; [291, 2026]; [294, 2026]; [057, 2026]; [058, 2026]; [059, 2026]; [060, 2026]; [301, 2026]; [298, 2026]; [302, 2026]; [297, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 11's source-canon section, directly verified anchors for the **Open-Source and Geospatial Intelligence Integrity** lane include [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]; [Agency, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples** and [253, 2026]; [255, 2026], but only directly verified source URLs are encoded as citations.

18.3.3.3 GEOINT and Imagery Intelligence intelligence practice lens: evidence artifact and safety check Practice lens: **Requirements-to-Evidence Lens** for **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**. [253, 2026]; [255, 2026].

Planning question: What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit?

Evidence artifact: requirements matrix with source descriptors, caveats, and collection limits.

Validation rule: show priority, authority, minimization, corroboration, and source quality before any claim is reused. Applied to **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**.

Handoff contract: deliver metadata-rich evidence packets, not unscoped data piles or implicit targeting requests.

Safety check: exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure.

18.3.3.4 GEOINT and Imagery Intelligence runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 18; [253, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	11.99	11.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind GEOINT and Imagery Intelligence to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Bounded autonomy, procurement, incident-response, and assurance studio	11.101	11.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for GEOINT and Imagery Intelligence	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Model-card, recoverability, retention, and learner-support evidence package	11.102	11.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for GEOINT and Imagery Intelligence	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Imagery quality literacy: resolution, temporal fit, and uncertainty	11.1	11.1 source title transformed into safe curriculum treatment; original: Geospatial Intelligence Fundamentals: IMINT, GEOINT, Mapping	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples	11.2	11.2 source title transformed into safe curriculum treatment; original: GEOINT Essential Body of Knowledge (USGIF)	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Imagery collection-platform literacy: resolution and revisit tradeoffs	11.3	11.3 source title transformed into safe curriculum treatment; original: Commercial Satellite Platforms: Maxar, Planet, Sentinel-1/2	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Claim-ledger memory exercise that tracks evidence changes rather than people	11.4	11.4 source title transformed into safe curriculum treatment; original: Change Detection and Pattern-of-Life Imagery Analysis	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples	11.5	11.5 source title transformed into safe curriculum treatment; original: GEOINT in Counterinsurgency and Strike Operations	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples	11.6	11.6 source title transformed into safe curriculum treatment; original: DoD GEOINT Accreditation and Training Standards	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples	11.7	11.7 source title transformed into safe curriculum treatment; original: MCRP 2-10B.4: USMC GEOINT Manual	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Imagery collection-platform literacy: resolution and revisit tradeoffs	11.8	11.8 source title transformed into safe curriculum treatment; original: AI-Assisted Satellite Image Analysis: Object Detection and Chronolocation	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples	11.9	11.9 source title transformed into safe curriculum treatment; original: Open-Source Geospatial Intelligence Library	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

18.3.3.5 GEOINT and Imagery Intelligence reusable subsection contract: topic rows, artifacts, and safety duties **Evidence anchor.** Section 18; [253, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Imagery quality literacy: resolution, temporal fit, and uncertainty	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Imagery collection-platform literacy: resolution and revisit tradeoffs	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Claim-ledger memory exercise that tracks evidence changes rather than people	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
GEOINT in Counterinsurgency and Strike: GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

Lesson topic	Practice lens	Evidence artifact	Safety check
DoD GEOINT Accreditation and Training: GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
MCRP 2-10B 4: GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
AI-Assisted Satellite Image Analysis: Imagery collection-platform literacy: resolution and revisit tradeoffs	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Open-Source Geospatial Intelligence Library: GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

18.3.3.6 GEOINT and Imagery Intelligence annotated source ledger: real titles and local contribution Each source cited by this **Open-Source and Geospatial Intelligence Integrity** module is paired below with its real title and a one-line note on what it contributes to **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**.

Source	Cited work	What it contributes	Status
[253, 2026]	Common European Data Spaces	This is an official European Commission webpage describing the Common European Data Spaces initiative, part of the EU strategy to create interconnected, trustworthy data-sharing environments across strategic sectors. It explains that data spaces let organizations and individuals share data while retaining control, guided by principles of open participation, privacy protection, and fair access rules.	verified source-guide
[255, 2026]	Web of Things (WoT) Architecture 1.1	The W3C Recommendation for Web of Things Architecture 1.1, published in December 2023, defining an abstract architecture for interoperability across diverse Internet of Things platforms. It introduces core concepts including Things described by machine-readable Thing Descriptions, reusable Thing Models, and Consumers that interpret descriptions to interact via Properties, Actions, and Events.	verified source-guide
[270, 2026]	NIST Big Data Interoperability Framework	NIST Special Publication 1500-1 (revised edition by Chang and Grady) establishes foundational terminology and consensus definitions for Big Data through the NIST Big Data Public Working Group. The volume defines Big Data characteristics, taxonomy, and a reference architecture assigning roles to Application Providers, Data Consumers, Data Providers, and System Orchestrators.	verified source-guide

Source	Cited work	What it contributes	Status
[278, 2026]	Recommendation of the Council on Public Procurement	The OECD Recommendation of the Council on Public Procurement (OECD/LEGAL/0411), a legal instrument adopted by the OECD Council in 2015 on the proposal of the Public Governance Committee. It frames public procurement as a pillar of strategic governance and service delivery and sets out principles for governments to follow.	verified source-guide
[279, 2026]	Open Contracting Data Standard	The documentation homepage for the Open Contracting Data Standard, version 1.1.5, maintained by the Open Contracting Partnership to support disclosure of government contracting data across the procurement lifecycle. It provides a common data model spanning planning, tender, award, contract, and implementation stages, along with a primer, implementation guidance, technical schemas, and validation tooling.	verified source-guide
[283, 2026]	Recommendation of the Council on Open Government	An OECD legal instrument document reproducing the Recommendation of the Council on Open Government (OECD/LEGAL/0438), adopted on 14 December 2017. It defines open government as a culture of governance promoting transparency, integrity, accountability, and stakeholder participation in support of democracy and inclusive growth.	verified source-guide
[290, 2026]	NIST SP 800-218A: Secure Software Development Practices for Generative AI and Dual-Use Foundation Models	NIST Special Publication 800-218A (July 2024), which augments the Secure Software Development Framework with practices specific to AI model development across the software lifecycle. Produced in response to Executive Order 14110, it addresses AI model producers, developers building on those models, and acquirers of AI systems, and is designed to be used alongside NIST SP 800-218.	verified source-guide
[291, 2026]	Revised 508 Standards and 255 Guidelines	Official documentation from the U.S. Access Board on the Revised 508 Standards and 255 Guidelines for information and communication technology accessibility. It establishes mandatory accessibility requirements for federal agencies and voluntary guidelines for telecommunications manufacturers, covering hardware, software, websites, electronic documents, and support services.	verified source-guide
[294, 2026]	M-25-21: Accelerating Federal Use of AI through Innovation, Governance, and Public Trust	An April 2025 Office of Management and Budget memorandum (M-25-21) directing executive branch agencies on federal use of artificial intelligence. Issued under Executive Order 14179, it instructs agencies to accelerate adoption of AI to improve public services and government efficiency while maintaining safeguards for civil rights, civil liberties, and privacy.	verified source-guide

Source	Cited work	What it contributes	Status
[057, 2026]	MCRP 2-10B.4 (SECURED) - Marines.mil	MCRP 2-10B.4 in the source guide links to the Marines GEOINT manual, not a reconnaissance manual. The linked PDF is 'Geospatial Intelligence Support to Operations'; verify the intended citation before reuse.	verified source-guide
[058, 2026]	GEOINT Essential Body of Knowledge	The GEOINT Essential Body of Knowledge (Version 2.0, 2019), published by the United States Geospatial Intelligence Foundation (USGIF). First developed in 2014 and revised with community input, it defines the competencies, standards, and learning objectives needed to succeed in the geospatial intelligence discipline.	verified source-guide
[059, 2026]	neonpangolin/geospatial-intelligence-library	A GitHub repository describing itself as a reference toolkit for geolocation and chronolocation in digital investigations. It curates open-source resources organized into categories including satellite imagery, mapping, infrastructure and transport tracking, weather and environmental monitoring, shadow and sun-position tools for time-of-day analysis, crisis and conflict mapping, image forensics, and geocoding utilities.	verified source-guide
[060, 2026]	DoDM 3305.10, "DoD Geospatial Intelligence (GEOINT	See bibliography for scope.	original source-guide
[301, 2026]	The IC OSINT Strategy 2024-2026	Official Intelligence Community strategy for open-source intelligence governance, integration, source discovery, data, tools, tradecraft, and workforce priorities.	original source-guide
[298, 2026]	Intelligence Community Directives	Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations.	original source-guide
[302, 2026]	National Geospatial-Intelligence Agency About Us	The official "About Us" page of the National Geospatial-Intelligence Agency (NGA), a U.S. Department of Defense and intelligence community organization. It describes NGA's mission of delivering geospatial intelligence, or GEOINT, to support military operations, policymakers, and first responders, spanning imagery analysis, mapping, geodesy, and navigation safety.	verified source-guide
[297, 2026]	Intelligence Community Directive 203: Analytic Standards	Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products.	original source-guide

Where this sits. This module's overview is Section 18; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

18.3.4 GEOINT and Imagery Intelligence governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 18; [253, 2026].

18.3.5 GEOINT and Imagery Intelligence analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 11's governance-boundary section, directly verified anchors for the **Open-Source and Geospatial Intelligence Integrity** lane include [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]; [Agency, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Research lane: **Open-Source and Geospatial Intelligence Integrity** for **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**. [253, 2026]; [255, 2026].
Curriculum topic spine: Imagery quality literacy: resolution, temporal fit, and uncertainty, **GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**, **Imagery collection-platform literacy: resolution and revisit tradeoffs**. **Verified anchor cluster:** [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]; [Agency, 2026b]; [for Standardization, 2013]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015].
Conceptual depth: public-source discovery converted into accountable intelligence through provenance, corroboration, minimization, and relevance tests.
Method stack: source triage, provenance capture, corroboration matrix, recency audit, geospatial context review, and confidence calibration.
Composability contract: collection notes, source metadata, transformations, caveats, and analytic judgments remain separately exportable.
Known failure modes: privacy drift, stale data, context collapse, platform bias, over-collection, and mistaking availability for reliability.
Defensive boundary: OSINT work uses lawful public, owned-lab, or explicitly approved sources and avoids doxxing, harassment, live tracking, or operational targeting. Applied to **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**.

Anchor	Why it matters here
[of the Director of National Intelligence and Agency, 2024]	Official IC OSINT strategy for professionalizing OSINT, integrated collection management, open-source sharing, innovation, and tradecraft. Checked as of 2026-05-21; role: curriculum_anchor.
[of State, 2024]	Official strategy source for lawful OSINT governance, discovery, validation, and dissemination. Checked as of 2026-05-21; role: curriculum_anchor.
[Agency, 2026c]	Official NGA strategy anchor for GEOINT readiness, warning, partnership resilience, resource stewardship, and AI integration. Checked as of 2026-05-21; role: curriculum_anchor.
[Agency, 2026b]	Official NGA source on GEOINT AI, data quality, model performance, interoperability, analyst interaction, and standards leadership. Checked as of 2026-05-21; role: curriculum_anchor.
[for Standardization, 2013]	International geospatial data-quality standard for completeness, logical consistency, positional accuracy, temporal quality, and usability framing. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026d]	Official sourcing directive for traceability, citations, source descriptors, and source summaries. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2015]	Official ODNI analytic tradecraft standards directive. Checked as of 2026-05-21; role: source_quality_anchor.

18.3.5.1 GEOINT and Imagery Intelligence evidence standard and citation floor: source families and discovery limits Official guidance supplies governance, safety, and legal constraints for the **Open-Source and Geospatial Intelligence Integrity** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [253, 2026]; [255, 2026].

18.3.6 GEOINT and Imagery Intelligence agentic boundary: assist, approve, block, and record

Evidence anchor. Section 18; [253, 2026].
AGEINT translation is bounded by the **Open-Source and Geospatial Intelligence Integrity** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**.

18.3.6.1 GEOINT and Imagery Intelligence permitted defensive utility: curriculum uses and safe outputs **Evidence anchor.** Section 18; [253, 2026].
The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**.

18.3.6.2 GEOINT and Imagery Intelligence excluded operational boundary: blocked actions and stop rules Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [253, 2026]; [255, 2026] and **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

18.3.7 GEOINT and Imagery Intelligence governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 18; [253, 2026].
Governance is practiced as a gate on the **Open-Source and Geospatial Intelligence Integrity** lane. Learners use the **Requirements-to-Evidence Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**.

18.3.7.1 GEOINT and Imagery Intelligence governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [253, 2026]; [255, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Open-Source and Geospatial Intelligence Integrity** failure modes and the **Requirements-to-Evidence Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

18.3.7.2 GEOINT and Imagery Intelligence evidence package handoff: appendices, records, and reuse

Evidence anchor. Section 18; [253, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Requirements-to-Evidence Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**.

18.3.7.3 GEOINT and Imagery Intelligence current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**. [253, 2026]; [255, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_ic_osint_strategy` for **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**?	The INT of First Resort: The IC OSINT Strategy 2024-2026; lane `osint_geoint`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official IC OSINT strategy for professionalizing OSINT, integrated collection management, open-source sharing, innovation, and tradecraft.
What does the module inherit from `official_state_osint_strategy` for **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**?	Open Source Intelligence Strategy; lane `osint_geoint`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official strategy source for lawful OSINT governance, discovery, validation, and dissemination.
What does the module inherit from `official_nga_strategy` for **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**?	NGA Strategy; lane `osint_geoint`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official NGA strategy anchor for GEOINT readiness, warning, partnership resilience, resource stewardship, and AI integration.
What does the module inherit from `official_nga_geoint_ai` for **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**?	GEOINT Artificial Intelligence; lane `osint_geoint`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official NGA source on GEOINT AI, data quality, model performance, interoperability, analyst interaction, and standards leadership.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 18; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

18.3.8 GEOINT and Imagery Intelligence assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 18; [253, 2026].

18.3.9 GEOINT and Imagery Intelligence assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 18; [253, 2026].

18.3.9.1 GEOINT and Imagery Intelligence capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples** and [253, 2026]; [255, 2026].

18.3.9.2 GEOINT and Imagery Intelligence instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples** and [253, 2026]; [255, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

18.3.9.3 GEOINT and Imagery Intelligence assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Imagery quality literacy: resolution, temporal fit, and uncertainty	Completed **requirements matrix with source descriptors, caveats, and collection limits** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples	Completed **requirements matrix with source descriptors, caveats, and collection limits** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Imagery collection-platform literacy: resolution and revisit tradeoffs	Completed **requirements matrix with source descriptors, caveats, and collection limits** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

18.3.10 GEOINT and Imagery Intelligence refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [253, 2026]; [255, 2026] and **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**.

18.3.10.1 GEOINT and Imagery Intelligence refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**. The local signals begin with [253, 2026]; [255, 2026].

18.3.10.2 GEOINT and Imagery Intelligence claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**, and the source spine for these checks begins with [253, 2026]; [255, 2026].

18.3.11 GEOINT and Imagery Intelligence reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [253, 2026]; [255, 2026].

Triangulation anchors. In module 11's review-checklist section, directly verified anchors for the **Open-Source and Geospatial Intelligence Integrity** lane include [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]; [Agency, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples**. [253, 2026]; [255, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

18.3.12 GEOINT and Imagery Intelligence learning-path links: module map, overview, and curriculum atlas

Use the cross-links below to place **Imagery quality literacy: resolution, temporal fit, and uncertainty; GEOINT data-quality audit using provided imagery metadata and non-sensitive synthetic change examples** in the wider unit: the orientation sets the frame, the parent unit supplies the shared safety posture, and the neighbouring modules show what evidence enters and leaves. Lead sources: [253, 2026]; [255, 2026].
Section 2, Section 15, Section 17, Section 19

19 TECHNICAL INTELLIGENCE AND CYBER OPERATIONS

19.1 TECHNICAL INTELLIGENCE AND CYBER OPERATIONS learning spine and source route: unit purpose, module order, and evidence handoff

Evidence anchor. Section 19; [258, 2026].

19.1.1 defensive cyber intelligence normalization discipline spine: domain question and learning focus

Evidence anchor. Section 19; [258, 2026].
This unit teaches **defensive cyber intelligence normalization**. Technical intelligence lessons normalize incidents, indicators, TTPs, supply-chain evidence, and sharing rules for defense and assurance.

19.1.2 defensive cyber intelligence normalization source-use contract: citation roles and evidence limits

Evidence anchor. Section 19; [258, 2026].
Use MITRE, NIST, CISA, STIX, and TAXII anchors for defensive taxonomy, secure development, sharing, and incident learning.

19.1.3 defensive cyber intelligence normalization practice artifact: recurring packet and retained evidence

Evidence anchor. Section 19; [258, 2026].
The recurring practice artifact is a **defensive CTI evidence packet** that draws on indicator context, TTP mapping, handling rule, and remediation owner. The unit keeps its learning spine explicit. Learners classify evidence defensively, state confidence, map controls, and preserve sharing restrictions.

19.1.4 defensive cyber intelligence normalization safety boundary: accountable, synthetic, and evidence-bounded limits

No exploit, persistence, evasion, scanning, or production response instructions.
This unit introduces the part's governing question, evidence artifacts, source-support spine, and capstone thread before the individual modules begin. [258, 2026]; [261, 2026].
Learners carry one unit capstone thread through the part: define an accountable intelligence question, bind it to source-quality constraints, produce a reviewable artifact, test the artifact against failure modes, and hand it off with enough context for another analyst or instructor to audit. The capstone remains public, synthetic, or owned-lab throughout; its first source anchors are [258, 2026]; [261, 2026].
This unit's deliverables are a source-canon card, claim/evidence ledger, safe-practice lab packet, failure-mode note, instructor rubric, and debrief memo. The full source-lane and evidence-package ledgers appear in the orientation and appendices; this unit introduction keeps only the learner-facing spine for [258, 2026]; [261, 2026].
This unit's safety gates are scope authorization, rights review, data provenance, tool allowlisting, human oversight, rollback, and evidence-bounded output. A missing gate turns the activity into a tabletop, audit, or written governance exercise until the gate is restored against [258, 2026]; [261, 2026].
Capstone thread:

Phase	Artifact	Review gate
Question	accountable learning question and excluded-action list	instructor confirms scope, allowed data, and rights impact
Source canon	source-lane map with guide citations, verified anchors, and refresh dates	citation keys resolve and source identity lock remains stable
Evidence ledger	claim, evidence, uncertainty, confidence, and reviewer register	every material claim has a source, caveat, and owner
Safe lab	synthetic or public dataset packet, tool allowlist, and stop conditions	no live target, private data, external action, or unsafe cyber-physical step
Assurance	evaluation rubric, failure-mode drill, rights map, and remediation note	human reviewer signs off before presentation or reuse
Debrief	capstone memo with lessons, residual risk, refresh triggers, and handoff owner	all unresolved questions and future approvals are explicit

Research lane: Governed Intelligence Cycle and Dissemination Architecture. Core anchors: [Community, 2026]; [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026c]. Conceptual focus: treating the intelligence cycle as a governed information system whose collection, processing, analysis, dissemination, evaluation, marking, and records obligations stay explicit. Composability contract: requirements, data provenance, analytic judgments, markings, dissemination permissions, records obligations, and feedback remain separable artifacts. **Practice lens:** Dissemination-and-Marking Control Lens; Which audience, release authority, marking vocabulary, records duty, and feedback loop governs this intelligence artifact? [258, 2026]; [261, 2026].

19.1.5 TECHNICAL INTELLIGENCE AND CYBER OPERATIONS visual navigation and module map: evidence flow, order, and safety cues

The unit uses Figure 52 and Figure 53 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 18, Section 20.

19.1.6 TECHNICAL INTELLIGENCE AND CYBER OPERATIONS module roster and source-lane inventory: citations, lanes, and learner route

Module	Section reference	Source spine
Cyber Intelligence Fundamentals	Section 20	[258, 2026]; [261, 2026]; [266, 2026]; [280, 2026]; [281, 2026]; [282, 2026]; [292, 2026]; [295, 2026]; [296, 2026]; [061, 2026]; [062, 2026]; [063, 2026]; [064, 2026]; [065, 2026]; [300, 2026]; [303, 2026]; [304, 2026]; [066, 2026]; [067, 2026]; [068, 2026]; [069, 2026]; [009, 2026]; [070, 2026]; [071, 2026].

Module	Section reference	Source spine
Advanced Persistent Threats (APTs)	Section 21	[237, 2026]; [258, 2026]; [261, 2026]; [273, 2026]; [276, 2026]; [285, 2026]; [286, 2026]; [290, 2026]; [294, 2026]; [072, 2026]; [069, 2026]; [071, 2026]; [300, 2026]; [303, 2026]; [304, 2026]; [309, 2026]; [310, 2026].
Supply Chain Intelligence Attacks	Section 22	[258, 2026]; [266, 2026]; [268, 2026]; [274, 2026]; [278, 2026]; [280, 2026]; [287, 2026]; [288, 2026]; [295, 2026]; [073, 2026]; [074, 2026]; [075, 2026]; [076, 2026]; [077, 2026]; [297, 2026]; [298, 2026]; [300, 2026]; [304, 2026]; [306, 2026].
Electronic and Emanations Intelligence	Section 23	[255, 2026]; [256, 2026]; [261, 2026]; [279, 2026]; [282, 2026]; [284, 2026]; [289, 2026]; [291, 2026]; [296, 2026]; [035, 2026]; [078, 2026]; [300, 2026]; [303, 2026]; [304, 2026]; [305, 2026]; [302, 2026]; [297, 2026].

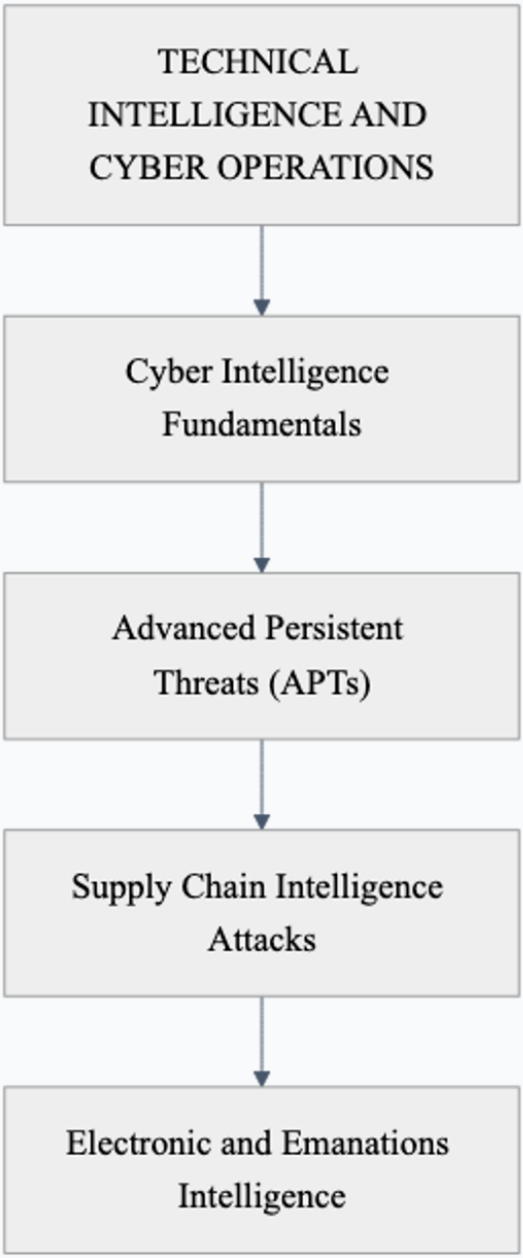


Figure 52: The unit module map traces the part's chapters as a linear reading sequence. It is anchored to the technical intelligence and cyber operations section; use it to inspect 4 module nodes in the unit's ordered, source-backed reading sequence from its first module to its last while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

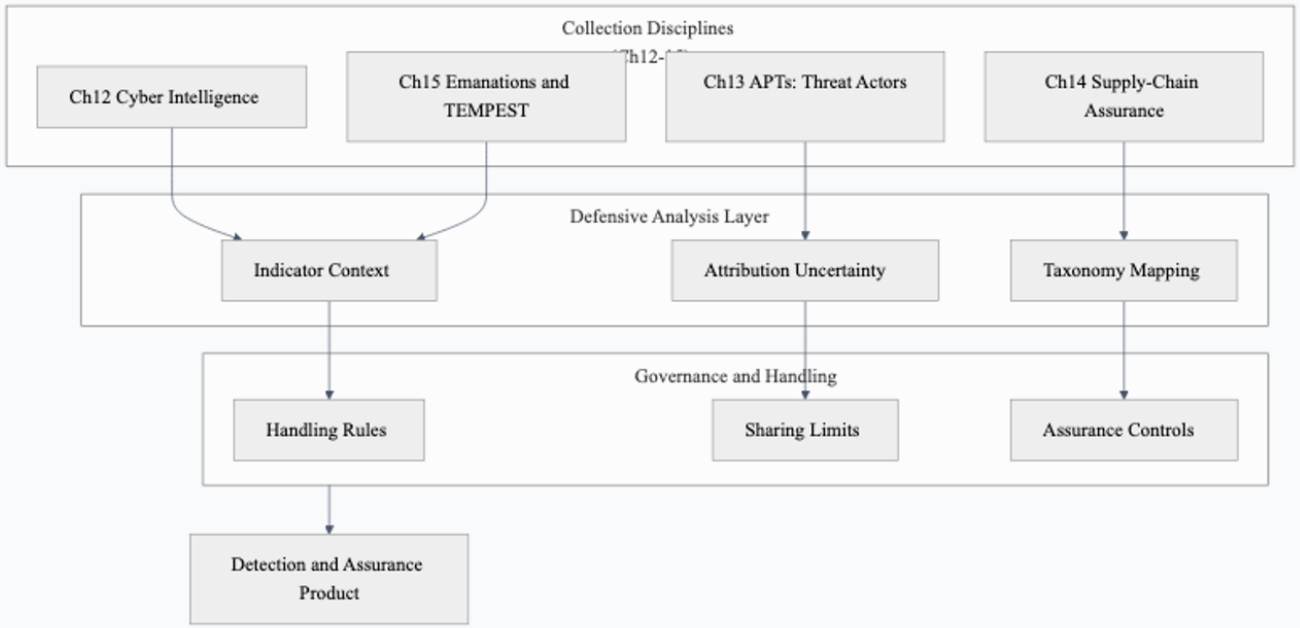


Figure 53: Each technical-collection discipline in this Part feeds a shared defensive pipeline that turns raw signals into governed detection, attribution, and assurance products. Its reader value is to make Collection Disciplines (Ch12-15), Ch12 Cyber Intelligence, Ch13 APTs: Threat Actors, and Ch14 Supply-Chain Assurance visible at a glance, with the technical intelligence and cyber operations section as the source section and defensive review as the boundary.

20 Cyber Intelligence Fundamentals

20.0.1 Cyber Intelligence Fundamentals figures and course links: visual evidence, source flow, and navigation

The module uses Figure 54 and Figure 52 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.

Navigation links: Section 2, Section 19, Section 21.

This module teaches the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane through a bounded, source-backed coursebook chapter. [258, 2026]; [261, 2026].

20.1 Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense frame for Cyber Intelligence Fundamentals: source context, topic focus, and reader task

Evidence anchor. Section 20; [258, 2026].

20.1.1 Cyber Intelligence Fundamentals orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 20; [258, 2026].

20.1.2 Cyber Intelligence Fundamentals conceptual primer: source context, core model, and reader task

This chapter teaches cyber threat intelligence as defensive normalization: incidents, indicators, TTPs, vendor risks, and sharing rules become useful only when scoped and validated. The chapter uses **Defensive Cyber-Intelligence Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**.

The central distinction is to separate defensive mapping and incident learning from exploit, persistence, or evasion instruction. Core topics include **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts; Reconnaissance through Resource Development: Cyber defensive taxonomy mapping using published labels and fabricated alerts**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.

Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [of Standards and Technology, 2016]; [Committee, 2025]; [Committee, 2021]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [258, 2026]; [261, 2026].

Learners move from vocabulary and the **Defensive Cyber-Intelligence Lens** distinction through topic lessons on **Cyber defensive taxonomy mapping using published labels and fabricated alerts** with evidence and misconception checks, then assemble a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** with safety and rights gates.

20.1.3 Cyber Intelligence Fundamentals learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 20; [258, 2026].

- Connect **Cyber defensive taxonomy mapping using published labels and fabricated alerts and MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts** to **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate defensive mapping and incident learning from exploit, persistence, or evasion instruction; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as indicator fixation, unvetted sharing, vendor-assurance drift, weak incident scoping, and treating CTI as a feed instead of a workflow, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: cyber material stays defensive and tabletop-based; it does not provide exploit, persistence, evasion, or live-response instructions.

20.1.4 Cyber Intelligence Fundamentals core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 20; [258, 2026].

Term	Working definition
Indicator	an observable signal that may support defensive detection or investigation
TTP	a tactic, technique, or procedure used for structured defensive mapping
Sighting	a bounded observation of a possible indicator in a given context
Handling rule	a sharing, marking, or retention limit for threat information
Lessons learned	the post-incident evidence that changes controls or playbooks
Cyber defensive taxonomy mapping using…	Key terms: Cyber, defensive, taxonomy.
MITRE ATT&CK Framework: Cyber defensive…	Key terms: MITRE, ATT, CK.

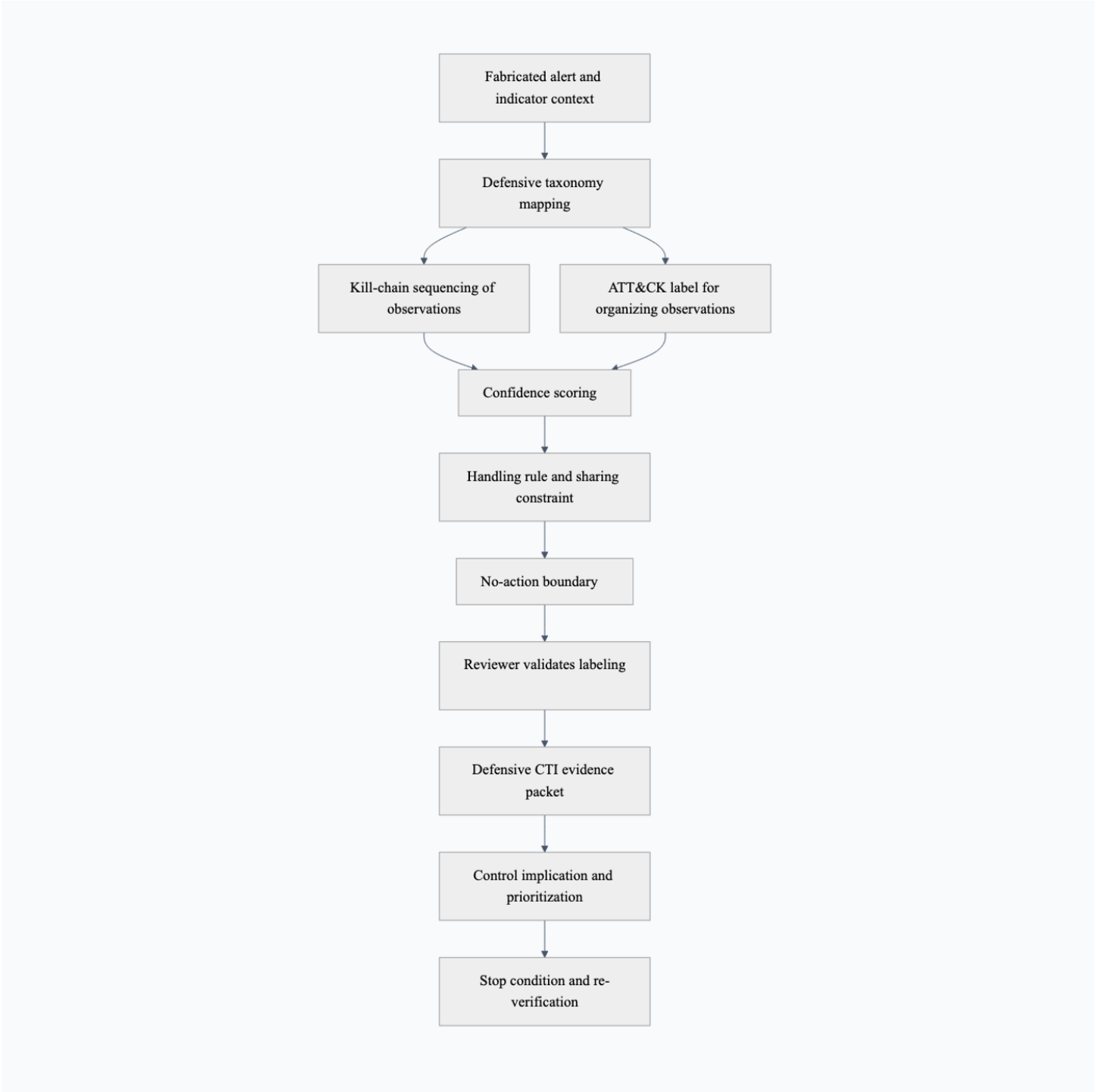


Figure 54: How fabricated alerts and published taxonomies are normalized into a defensive intelligence packet with confidence and control implications, never an action sequence. In the technical intelligence and cyber operations / cyber intelligence fundamentals section, it lets readers compare Fabricated alert and indicator context, Defensive taxonomy mapping, Kill-chain sequencing of observations, and ATT&CK label for organizing observations so the visual functions as a traceable course aid rather than an unscoped assertion.

20.2 Defensive Cyber-Intelligence Lens path for Cyber Intelligence Fundamentals: lesson cluster, safe artifact, and review

Evidence anchor. Section 20; [258, 2026].

20.2.1 Cyber Intelligence Fundamentals practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 20; [258, 2026].

20.2.2 Cyber Intelligence Fundamentals topic lessons: source-backed concepts and transfer tasks

This module builds cyber threat intelligence as defensive normalization: incidents, indicators, TTPs, vendor risks, and sharing rules become useful only when scoped and validated. The sequence opens with **Cyber defensive taxonomy mapping using published labels and fabricated alerts**, **MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**, **Reconnaissance through Resource Development: Cyber defensive taxonomy mapping using published labels and fabricated alerts** and applies the **Defensive Cyber-Intelligence Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 52; module overview Section 20; curriculum atlas Section 2.

Triangulation anchors. In module 12's topic-lessons section, directly verified anchors for the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane include [of Standards and Technology, 2016]; [Committee, 2025]; [Committee, 2021]; [MITRE, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

20.2.2.1 Lesson 1: Cyber defensive taxonomy mapping using published labels and fabricated alerts **Concept. Cyber defensive taxonomy mapping using published labels and fabricated alerts** uses the model as defensive vocabulary for sequencing observations, not as a checklist of adversary actions.

Why it matters. Analysts use **Cyber defensive taxonomy mapping** to separate defensive mapping and incident learning from exploit, persistence, or evasion instruction. A defensible treatment names the judgment it enables for defensive CTI normalization and tabletop incident learning review, the proof limit that treating defensive taxonomy labels as an action sequence would otherwise hide, and the reviewer accountable for challenge.

Source support. Cyber defensive taxonomy mapping using published labels and fabricated alerts rests on [061, 2026] and [062, 2026]. The most specific cited work observes: This Lockheed Martin webpage describes the Cyber Kill Chain framework, a methodology for identifying and preventing cyber intrusions as part of the company's Intelligence Driven Defense model. Use them for the claim that **Cyber defensive taxonomy mapping using published labels and fabricated alerts** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. For **Cyber defensive taxonomy mapping**, work from the cited evidence behind this row. [061, 2026] This Lockheed Martin webpage describes the Cyber Kill Chain framework, a methodology for identifying and preventing cyber intrusions as part of the company's Intelligence Driven Defense model. It outlines the sequence of steps an adversary must complete to achieve an objective, and is intended to help analysts understand attacker tactics and procedures. [062, 2026] A Wikipedia article describing the cyber kill chain, a framework adapted by Lockheed Martin from a military concept to model how cyberattacks progress through distinct phases. It outlines seven stages from reconnaissance through actions on objectives, along with defensive countermeasures organizations can apply at each stage. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Cyber defensive taxonomy mapping**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this defensive CTI normalization and tabletop incident learning topic. The artifact must map the indicator descriptor, the bounded claim about **Cyber defensive taxonomy mapping using**, the taxonomy caveat, the confidence note, the no-action boundary, and the reviewer who validates the labeling. Shape **Cyber defensive taxonomy mapping** work as a **defensive CTI evidence packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that a defensive taxonomy is an instruction sequence.

Transfer task. Transfer **Cyber defensive taxonomy mapping** from this module to a second motif by preserving defensive CTI normalization and tabletop incident learning, replacing action with audit, and naming the blocked use.

20.2.2.2 Lesson 2: MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts **Concept. MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts** uses the taxonomy label to organize fabricated defensive observations, confidence, and control implications without describing adversary execution.

Why it matters. Without explicit treatment of **MITRE ATT&CK Framework**, treating defensive taxonomy labels as an action sequence undermines defensive CTI normalization and tabletop incident learning review; the lesson builds the habit to separate defensive mapping and incident learning from exploit, persistence, or evasion instruction.

Source support. MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts rests on [063, 2026] and [064, 2026]. The lead source's own note reads: The official MITRE ATT&CK Enterprise Matrix, a curated knowledge base of adversary tactics and techniques observed in real-world intrusions. Use them for fixing what **MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. Ground **MITRE ATT&CK Framework** in the evidence the row cites. [063, 2026] The official MITRE ATT&CK Enterprise Matrix, a curated knowledge base of adversary tactics and techniques observed in real-world intrusions. It organizes activity into fifteen sequential tactics, from reconnaissance and resource development through initial access, persistence, privilege escalation, defense evasion, credential access, lateral movement, command and control, exfiltration, and impact. [064, 2026] MITRE ATT&CK is a globally accessible knowledge base that catalogs adversary tactics and techniques drawn from real-world observations of cyber intrusions. The framework is organized into matrices covering Enterprise, Mobile, and Industrial Control Systems environments, with tactics representing adversary objectives and techniques describing specific methods used to achieve them. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **MITRE ATT&CK Framework**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this defensive CTI normalization and tabletop incident learning topic. The artifact must map the indicator descriptor, the bounded claim about **MITRE ATT&CK Framework**, the taxonomy caveat, the confidence note, the no-action boundary, and the reviewer who validates the labeling. Shape **MITRE ATT&CK Framework** work as a **defensive CTI evidence packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that a defensive taxonomy label is an action sequence rather than a vocabulary for describing and detecting behavior.

Transfer task. Transfer **MITRE ATT&CK Framework** from this module to a second motif by preserving defensive CTI normalization and tabletop incident learning, replacing action with audit, and naming the blocked use.

20.2.2.3 Lesson 3: Reconnaissance through Resource Development: Cyber defensive taxonomy mapping using published labels and fabricated alerts **Concept. Reconnaissance through Resource Development: Cyber defensive taxonomy mapping using published**

labels and fabricated alerts uses the taxonomy label to organize fabricated defensive observations, confidence, and control implications without describing adversary execution.

Why it matters. Analysts use **Reconnaissance through Resource Development** to separate defensive mapping and incident learning from exploit, persistence, or evasion instruction. A defensible treatment names the judgment it enables for defensive CTI normalization and tabletop incident learning review, the proof limit that treating defensive taxonomy labels as an action sequence would otherwise hide, and the reviewer accountable for challenge.

Source support. Reconnaissance through Resource Development: Cyber defensive taxonomy mapping using published labels and fabricated alerts rests on [063, 2026]. Its anchor reference records: The official MITRE ATT&CK Enterprise Matrix, a curated knowledge base of adversary tactics and techniques observed in real-world intrusions. Use it for the working definition that **Reconnaissance through Resource Development: Cyber defensive taxonomy mapping using published labels and fabricated alerts** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. For **Reconnaissance through Resource Development**, work from the cited evidence behind this row. [063, 2026] The official MITRE ATT&CK Enterprise Matrix, a curated knowledge base of adversary tactics and techniques observed in real-world intrusions. It organizes activity into fifteen sequential tactics, from reconnaissance and resource development through initial access, persistence, privilege escalation, defense evasion, credential access, lateral movement, command and control, exfiltration, and impact. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Reconnaissance through Resource Development**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this defensive CTI normalization and tabletop incident learning topic. The artifact must map the indicator descriptor, the bounded claim about **Reconnaissance through Resource Development**, the taxonomy caveat, the confidence note, the no-action boundary, and the reviewer who validates the labeling. Shape **Reconnaissance through Resource Development** work as a **defensive CTI evidence packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that a defensive taxonomy label is an action sequence rather than a vocabulary for describing and detecting behavior.

Transfer task. Apply this module's safe boundary for **Reconnaissance through Resource Development** to another artifact while keeping defensive CTI normalization and tabletop incident learning and reviewer ownership explicit.

20.2.2.4 Lesson 4: Cyber access-and-execution taxonomy review using fabricated alerts

Concept. Cyber access-and-execution taxonomy review using fabricated alerts uses the taxonomy label to organize fabricated defensive observations, confidence, and control implications without describing adversary execution.

Why it matters. Analysts use **Cyber access-and-execution taxonomy review** to separate defensive mapping and incident learning from exploit, persistence, or evasion instruction. A defensible treatment names the judgment it enables for defensive CTI normalization and tabletop incident learning review, the proof limit that treating defensive taxonomy labels as an action sequence would otherwise hide, and the reviewer accountable for challenge.

Source support. Cyber access-and-execution taxonomy review using fabricated alerts rests on [065, 2026]. The most specific cited work observes: The Enterprise Techniques page of the MITRE ATT&CK framework, a cybersecurity knowledge base maintained by MITRE Corporation. Use it for fixing what **Cyber access-and-execution taxonomy review using fabricated alerts** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. For **Cyber access-and-execution taxonomy review**, reason from the sources cited in this row. [065, 2026] The Enterprise Techniques page of the MITRE ATT&CK framework, a cybersecurity knowledge base maintained by MITRE Corporation. It documents 222 enterprise techniques and 475 sub-techniques describing how adversaries achieve tactical goals across the attack lifecycle, organized by tactics such as initial access, persistence, privilege escalation, defense evasion, credential access, discovery, and impact. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Cyber access-and-execution taxonomy review**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this defensive CTI normalization and tabletop incident learning topic. The artifact must map the indicator descriptor, the bounded claim about **Cyber access-and-execution taxonomy review using**, the taxonomy caveat, the confidence note, the no-action boundary, and the reviewer who validates the labeling. Shape **Cyber access-and-execution taxonomy review** work as a **defensive CTI evidence packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Cyber access-and-execution taxonomy review**: that a defensive taxonomy label is an action sequence rather than a vocabulary for describing and detecting behavior.

Transfer task. Apply this module's safe boundary for **Cyber access-and-execution taxonomy review** to another artifact while keeping defensive CTI normalization and tabletop incident learning and reviewer ownership explicit.

20.2.2.5 Lesson 5: Cyber credential-and-movement taxonomy review using fabricated alerts

Concept. Cyber credential-and-movement taxonomy review using fabricated alerts uses the taxonomy label to organize fabricated defensive observations, confidence, and control implications without describing adversary execution.

Why it matters. Cyber credential-and-movement taxonomy review connects classroom vocabulary to Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Cyber credential-and-movement taxonomy review using fabricated alerts rests on [300, 2026], [303, 2026], and [304, 2026]. The most specific cited work observes: An official NIST page on software supply chain security issued under Executive Order 14028, focused on the Software Bill of Materials as a formal record of software components and their supply chain. Use them for the working definition that **Cyber credential-and-movement taxonomy review using fabricated alerts** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. For **Cyber credential-and-movement taxonomy review**, reason from the sources cited in this row. [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. [303, 2026] An official NIST page on software supply chain security issued under Executive Order 14028, focused on the Software Bill of Materials as a formal record of software components and their supply chain. It explains the benefits of SBOMs for vulnerability identification and supply-chain transparency, recommends machine-readable formats such as SPDX, CycloneDX, and SWID, and describes foundational, sustaining, and enhancing levels of implementation. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Cyber credential-and-movement taxonomy review**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this defensive CTI normalization and tabletop incident learning topic. The artifact must map the indicator descriptor, the bounded claim about **Cyber credential-and-movement taxonomy review using**, the taxonomy caveat, the confidence note, the no-action boundary, and the reviewer who validates the labeling. Shape **Cyber credential-and-movement taxonomy review** work as a **defensive CTI evidence packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Cyber credential-and-movement taxonomy review**: that a defensive taxonomy label is an action sequence rather than a vocabulary for describing and detecting behavior.

Transfer task. Transfer **Cyber credential-and-movement taxonomy review** from this module to a second motif by preserving defensive CTI normalization and tabletop incident learning, replacing action with audit, and naming the blocked use.

20.2.2.6 Lesson 6: Cyber command, data-loss, and impact taxonomy review using fabricated alerts

Concept. Cyber command, data-loss, and impact taxonomy review using fabricated alerts uses the taxonomy label to organize fabricated defensive observations, confidence, and control implications without describing adversary execution.

Why it matters. Cyber command, data-loss, and impact taxonomy review using fabricated alerts matters in the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane because defensive CTI normalization and tabletop incident learning evidence must stay separate from judgment; treating defensive taxonomy labels as an action sequence is a common failure.

Source support. Cyber command, data-loss, and impact taxonomy review using fabricated alerts rests on [062, 2026] and [063, 2026]. Its anchor reference records: The official MITRE ATT&CK Enterprise Matrix, a curated knowledge base of adversary tactics and techniques observed in real-world intrusions. Use them for pinning down the scope of **Cyber command, data-loss, and impact taxonomy review using fabricated alerts**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. For **Cyber command, data-loss, and impact taxonomy review using fabricated alerts**, work from the cited evidence behind this row. [062, 2026] A Wikipedia article describing the cyber kill chain, a framework adapted by Lockheed Martin from a military concept to model how cyberattacks progress through distinct phases. It outlines seven stages from reconnaissance through actions on objectives, along with defensive countermeasures organizations can apply at each stage. [063, 2026] The official MITRE ATT&CK Enterprise Matrix, a curated knowledge base of adversary tactics and techniques observed in real-world intrusions. It organizes activity into fifteen sequential tactics, from reconnaissance and resource development through initial access, persistence, privilege escalation, defense evasion, credential access, lateral movement, command and control, exfiltration, and impact. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Cyber command, data-loss, and impact taxonomy review using fabricated alerts**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this defensive CTI normalization and tabletop incident learning topic. The artifact must map the indicator descriptor, the bounded claim about **Cyber command data-loss and impact**, the taxonomy caveat, the confidence note, the no-action boundary, and the reviewer who validates the labeling. Shape this subject work as a **defensive CTI evidence packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Cyber command, data-loss, and impact taxonomy review using fabricated alerts**: that a defensive taxonomy label is an action sequence rather than a vocabulary for describing and detecting behavior.

Transfer task. Apply this module's safe boundary for **Cyber command, data-loss, and impact taxonomy review using fabricated alerts** to another artifact while keeping defensive CTI normalization and tabletop incident learning and reviewer ownership explicit.

20.2.2.7 Lesson 7: Unified Kill Chain: Cyber defensive taxonomy mapping using published labels and fabricated alerts

Concept. Unified Kill Chain: Cyber defensive taxonomy mapping using published labels and fabricated alerts uses the model as defensive vocabulary for sequencing observations, not as a checklist of adversary actions.

Why it matters. Unified Kill Chain matters in the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane because defensive CTI normalization and tabletop incident learning evidence must stay separate from judgment; treating defensive taxonomy labels as an action sequence is a common failure.

Source support. Unified Kill Chain: Cyber defensive taxonomy mapping using published labels and fabricated alerts rests on [062, 2026]. The closest source to this row notes: It outlines seven stages from reconnaissance through actions on objectives, along with defensive countermeasures organizations can apply at each stage. Use it for fixing what **Unified Kill Chain: Cyber defensive taxonomy mapping using published labels and fabricated alerts** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. For **Unified Kill Chain**, work from the cited evidence behind this row. [062, 2026] A Wikipedia article describing the cyber kill chain, a framework adapted by Lockheed Martin from a military concept to model how cyberattacks progress through distinct phases. It outlines seven stages from reconnaissance through actions on objectives, along with defensive countermeasures organizations can apply at each stage. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Unified Kill Chain**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this defensive CTI normalization and tabletop incident learning topic. The artifact must map the indicator descriptor, the bounded claim about **Unified Kill Chain**, the taxonomy caveat, the confidence note, the no-action boundary, and the reviewer who validates the labeling. Shape **Unified Kill Chain** work as a **defensive CTI evidence packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that a defensive taxonomy is an instruction sequence.

Transfer task. Transfer **Unified Kill Chain** from this module to a second motif by preserving defensive CTI normalization and tabletop incident learning, replacing action with audit, and naming the blocked use.

20.2.2.8 Lesson 8: Threat Intelligence Sharing: Cyber defensive taxonomy mapping using published labels and fabricated alerts

Concept. Threat Intelligence Sharing: Cyber defensive taxonomy mapping using published labels and fabricated alerts uses sharing standards to document indicator context, handling, confidence, and consumer responsibilities—not raw indicator hoarding.

Why it matters. Without explicit treatment of **Threat Intelligence Sharing**, treating defensive taxonomy labels as an action sequence undermines defensive CTI normalization and tabletop incident learning review; the lesson builds the habit to separate defensive mapping and incident learning from exploit, persistence, or evasion instruction.

Source support. Threat Intelligence Sharing: Cyber defensive taxonomy mapping using published labels and fabricated alerts rests on [066, 2026], [067, 2026], and [068, 2026]. The most specific cited work observes: STIX defines a structured language for representing threat information, while TAXII specifies how that information is transported and exchanged between systems. Use them for fixing what **Threat Intelligence Sharing: Cyber defensive taxonomy mapping using published labels and fabricated alerts** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. Ground **Threat Intelligence Sharing** in the evidence the row cites. [066, 2026] A Cloudflare Learning Center explainer describing STIX and TAXII as complementary standards for cyber threat intelligence. STIX defines a structured language for representing threat information, while TAXII specifies how that information is transported and exchanged between systems. Together they form a framework that lets organizations share and consume threat intelligence in a consistent, machine-readable way to improve collective defense. [067, 2026] An introductory page from the OASIS CTI documentation explaining STIX (Structured Threat Information Expression), an open-source language and serialization format used to exchange cyber threat intelligence. It describes how STIX 2.1 models intelligence using 18 domain objects (such as attack patterns, malware, threat actors, and vulnerabilities) and 2 relationship objects, all represented as JSON. [068, 2026] The official committee page for the OASIS Cyber Threat Intelligence (CTI) Technical Committee, a standards body that develops formats for sharing cyber threat intelligence. It maintains the STIX (Structured Threat Information Expression) data model and the TAXII exchange protocol, both approved as OASIS standards in 2021, and organizes subcommittees for STIX, TAXII, and interoperability. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Threat Intelligence Sharing**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this defensive CTI normalization and tabletop incident learning topic. The artifact must map the indicator descriptor, the bounded claim about **Threat Intelligence Sharing**, the taxonomy caveat, the confidence note, the no-action boundary, and the reviewer who validates the labeling. Shape **Threat Intelligence Sharing** work as a **defensive CTI evidence packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that a defensive taxonomy label is an action sequence rather than a vocabulary for describing and detecting behavior.

Transfer task. Transfer **Threat Intelligence Sharing** from this module to a second motif by preserving defensive CTI normalization and tabletop incident learning, replacing action with audit, and naming the blocked use.

20.2.2.9 Lesson 9: Nation-State Cyber Espionage: Cyber defensive taxonomy mapping using published labels and fabricated alerts

Concept. Nation-State Cyber Espionage: Cyber defensive taxonomy mapping using published labels and fabricated alerts uses the taxonomy label to organize fabricated defensive observations, confidence, and control implications without describing adversary execution.

Why it matters. Nation-State Cyber Espionage connects classroom vocabulary to Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Nation-State Cyber Espionage: Cyber defensive taxonomy mapping using published labels and fabricated alerts rests on [069, 2026]. The closest source to this row notes: They found that the most common cyberattacks initiated by nation-states were espionage focused. Use it for pinning down the scope of **Nation-State Cyber Espionage: Cyber defensive taxonomy mapping using published labels and fabricated alerts**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. For **Nation-State Cyber Espionage**, work from the cited evidence behind this row. [069, 2026] They found that the most common cyberattacks initiated by nation-states were espionage focused. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Nation-State Cyber Espionage**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this defensive CTI normalization and tabletop incident learning topic. The artifact must map the indicator descriptor, the bounded claim about **Nation-State Cyber Espionage**, the taxonomy caveat, the confidence note, the no-action boundary, and the reviewer who validates the labeling. Shape **Nation-State Cyber Espionage** work as a **defensive CTI evidence packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that a defensive taxonomy label is an action sequence rather than a vocabulary for describing and detecting behavior.

Transfer task. Transfer **Nation-State Cyber Espionage** from this module to a second motif by preserving defensive CTI normalization and tabletop incident learning, replacing action with audit, and naming the blocked use.

20.2.2.10 Lesson 10: Chinese State-Affiliated Hacking: Cyber defensive taxonomy mapping using published labels and fabricated alerts

Concept. Chinese State-Affiliated Hacking: Cyber defensive taxonomy mapping using published labels and fabricated alerts uses the taxonomy label to organize fabricated defensive observations, confidence, and control implications without describing adversary execution.

Why it matters. Analysts use **Chinese State-Affiliated Hacking** to separate defensive mapping and incident learning from exploit, persistence, or evasion instruction. A defensible treatment names the judgment it enables for defensive CTI normalization and tabletop incident learning review, the proof limit that treating defensive taxonomy labels as an action sequence would otherwise hide, and the reviewer accountable for challenge.

Source support. Chinese State-Affiliated Hacking: Cyber defensive taxonomy mapping using published labels and fabricated alerts rests on [009, 2026] and [070, 2026]. The most specific cited work observes: Organized in three parts, it surveys China-US relations in the cyber domain and the policy dilemmas of attribution and shared terminology, presents a case study of the APT1 hacker group linked to PLA Unit 61398, and reviews broader trends in the context of the 2015 US-China Cyber Agreement. Use them for the working definition that **Chinese State-Affiliated Hacking: Cyber defensive taxonomy mapping using published labels and fabricated alerts** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. Ground **Chinese State-Affiliated Hacking** in the evidence the row cites. [009, 2026] A November 2023 report from MERICS (Mercator Institute for China Studies) analyzing Chinese state-affiliated cyber intrusions aimed at strategic goals. It argues that Chinese actors pursue long-term, persistent access to European technology firms and critical infrastructure for espionage rather than disruption, with targeting aligned to government priorities such as semiconductors, pharmaceuticals, and advanced manufacturing. [070, 2026] A 2016 student security paper by Winnona DeSombre (Tufts Comp116) analyzing the evolution of China's cyber espionage campaigns against the United States. Organized in three parts, it surveys China-US relations in the cyber domain and the policy dilemmas of attribution and shared terminology, presents a case study of the APT1 hacker group linked to PLA Unit 61398, and reviews broader trends in the context of the 2015 US-China Cyber Agreement. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Chinese State-Affiliated Hacking**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this defensive CTI normalization and tabletop incident learning topic. The artifact must map the indicator descriptor, the bounded claim about **Chinese State-Affiliated Hacking**, the taxonomy caveat, the confidence note, the no-action boundary, and the reviewer who validates the labeling. Shape **Chinese State-Affiliated Hacking** work as a **defensive CTI evidence packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that a defensive taxonomy label is an action sequence rather than a vocabulary for describing and detecting behavior.

Transfer task. Apply this module's safe boundary for **Chinese State-Affiliated Hacking** to another artifact while keeping defensive CTI normalization and tabletop incident learning and reviewer ownership explicit.

20.2.2.11 Lesson 11: Russian Cyber Operations: Cyber defensive taxonomy mapping using published labels and fabricated alerts

Concept. Russian Cyber Operations: Cyber defensive taxonomy mapping using published labels and fabricated alerts uses the taxonomy label to organize fabricated defensive observations, confidence, and control implications without describing adversary execution.

Why it matters. Russian Cyber Operations connects classroom vocabulary to Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Russian Cyber Operations: Cyber defensive taxonomy mapping using published labels and fabricated alerts rests on [300, 2026], [303, 2026], and [304, 2026]. The closest source to this row notes: It explains the benefits of SBOMs for vulnerability identification and supply-chain transparency, recommends machine-readable formats such as SPDX, CycloneDX, and SWID, and describes foundational, sustaining, and enhancing levels of implementation. Use them for pinning down the scope of **Russian Cyber Operations: Cyber defensive taxonomy mapping using published labels and fabricated alerts**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. Read **Russian Cyber Operations** against the works cited for this row. [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. [303, 2026] An official NIST page on software supply chain security issued under Executive Order 14028, focused on the Software Bill of Materials as a formal record of software components and their supply chain. It explains the benefits of SBOMs for vulnerability identification and supply-chain transparency, recommends machine-readable formats

such as SPDX, CycloneDX, and SWID, and describes foundational, sustaining, and enhancing levels of implementation. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Russian Cyber Operations**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this defensive CTI normalization and tabletop incident learning topic. The artifact must map the indicator descriptor, the bounded claim about **Russian Cyber Operations**, the taxonomy caveat, the confidence note, the no-action boundary, and the reviewer who validates the labeling. Shape **Russian Cyber Operations** work as a **defensive CTI evidence packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that a defensive taxonomy label is an action sequence rather than a vocabulary for describing and detecting behavior.

Transfer task. Reuse the **Russian Cyber Operations** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

20.2.2.12 Lesson 12: Living-Off-The-Land Techniques in APT Operations: Cyber defensive taxonomy mapping using published labels and fabricated alerts Concept. Living-Off-The-Land Techniques in APT Operations: Cyber defensive taxonomy mapping using published labels and fabricated alerts

Living-Off-The-Land Techniques in APT Operations: Cyber defensive taxonomy mapping using published labels and fabricated alerts studies APT reporting as attribution and confidence literacy: technical similarity, context, caveats, and geopolitical inference stay separate.

Why it matters. Analysts use **Living-Off-The-Land Techniques in APT Operations** to separate defensive mapping and incident learning from exploit, persistence, or evasion instruction. A defensible treatment names the judgment it enables for defensive CTI normalization and tabletop incident learning review, the proof limit that treating defensive taxonomy labels as an action sequence would otherwise hide, and the reviewer accountable for challenge.

Source support. Living-Off-The-Land Techniques in APT Operations: Cyber defensive taxonomy mapping using published labels and fabricated alerts rests on [071, 2026]. Its anchor reference records: Attribution becomes harder when its open-source … Use it for the working definition that **Living-Off-The-Land Techniques in APT Operations: Cyber defensive taxonomy mapping using published labels and fabricated alerts** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. Ground **Living-Off-The-Land Techniques in APT Operations** in the evidence the row cites. [071, 2026] Attribution becomes harder when its open-source … Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Living-Off-The-Land Techniques in APT Operations**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this defensive CTI normalization and tabletop incident learning topic. The artifact must map the indicator descriptor, the bounded claim about **Living-Off-The-Land Techniques in APT Operations**, the taxonomy caveat, the confidence note, the no-action boundary, and the reviewer who validates the labeling. Shape **Living-Off-The-Land Techniques in APT Operations** work as a **defensive CTI evidence packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that a defensive taxonomy label is an action sequence rather than a vocabulary for describing and detecting behavior.

Transfer task. Reuse the **Living-Off-The-Land Techniques in APT Operations** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

20.2.3 Cyber Intelligence Fundamentals worked safe example: synthetic inputs, evidence, and review

Worked example: a sample campus SOC reviews fabricated alert records after a tabletop incident. [258, 2026]; [261, 2026].

Triangulation anchors. In module 12's worked-example section, directly verified anchors for the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane include [of Standards and Technology, 2016]; [Committee, 2025]; [Committee, 2021]; [MITRE, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **defensive cyber intelligence normalization**. Learners use a **defensive CTI evidence packet** and keep this boundary visible: No exploit, persistence, evasion, scanning, or production response instructions.

Frame. The classroom question centers on **Cyber defensive taxonomy mapping using published labels and fabricated alerts**. Excluded actions stay explicit, and the **Defensive Cyber-Intelligence Lens** planning question is: Which defensive observation, confidence level, handling rule, and control implication can be stated without teaching adversary action?

Inputs. For the **Cyber defensive taxonomy mapping using published labels and fabricated alerts** scenario, use toy alerts, synthetic asset names, public ATT&CK technique descriptions, and a sharing-policy card. The Defensive Cyber-Intelligence Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Cyber defensive taxonomy mapping using published labels and fabricated alerts**, students normalize indicators, map TTPs defensively, rate confidence, mark sharing limits, and record lessons learned. Pause whenever an inference about Cyber defensive taxonomy mapping using published labels and fabricated alerts appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Cyber defensive taxonomy mapping using published labels and fabricated alerts** classroom scenario; unit artifact = defensive CTI evidence packet; evidence = allowed inputs; method = defensive CTI normalization and tabletop incident learning; output = a CTI packet with indicators, TTP mapping, confidence, handling rule, and remediation owner; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Cyber defensive taxonomy mapping using published labels and fabricated alerts** as "Defensive Cyber-Intelligence Lens confirms it" is not enough. The revision ties the claim to defensive CTI normalization and tabletop incident learning, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Cyber defensive taxonomy mapping using published labels and fabricated alerts** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

20.2.4 Cyber Intelligence Fundamentals practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Defensive Cyber-Intelligence Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**.

Triangulation anchors. In module 12's practice-sequence section, directly verified anchors for the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane include [of Standards and Technology, 2016]; [Committee, 2025]; [Committee, 2021]; [MITRE, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Cyber defensive taxonomy mapping using published labels and fabricated alerts, MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts, Reconnaissance through Resource Development: Cyber defensive taxonomy mapping using published labels and fabricated alerts; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane.
2. Frame	Answer the lens question: Which defensive observation, confidence level, handling rule, and control implication can be stated without teaching adversary action?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Cyber defensive taxonomy mapping using published labels and fabricated alerts: defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the defensive CTI evidence packet fields for Cyber defensive taxonomy mapping using published labels and fabricated alerts.	Unit profile note.	Evidence artifacts include indicator context, TTP mapping.
4. Challenge	Test the misconception that a defensive taxonomy is an instruction sequence.	Failure-mode note.	The artifact applies the key distinction: separate defensive mapping and incident learning from exploit, persistence, or evasion instruction.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

20.2.4.1 Cyber Intelligence Fundamentals instructor notes: source reasoning, review points, and studio focus Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**. [258, 2026]; [261, 2026].

20.2.4.2 Cyber Intelligence Fundamentals extension exercise: peer validation and refresh trigger review **Evidence anchor.** Section 20; [258, 2026].

Have learners swap artifacts and apply the **Defensive Cyber-Intelligence Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**.

20.2.5 Cyber Intelligence Fundamentals knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 20; [258, 2026].

1. Explain how **Cyber defensive taxonomy mapping using published labels and fabricated alerts** is defined here; name the source descriptor that supports the definition.
2. Contrast **Cyber defensive taxonomy mapping using published labels and fabricated alerts** with **MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts** using the **Defensive Cyber-Intelligence Lens** artifact fields.
3. Identify one failure mode from the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which indicator is useful only after context and confidence are added?
5. Correct this misconception: that a defensive taxonomy is an instruction sequence.

20.2.5.1 Cyber Intelligence Fundamentals answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Cyber defensive taxonomy mapping using published labels and fabricated alerts** without source evidence, uncertainty, or a safe transfer task.

20.3 Cyber Intelligence Fundamentals assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 20; [258, 2026].

20.3.1 Cyber Intelligence Fundamentals evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 20; [258, 2026].

20.3.2 Cyber Intelligence Fundamentals transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 20; [258, 2026].

20.3.2.1 Cyber Intelligence Fundamentals lineage and source tradition: profile, concepts, and first anchors This sits in the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lineage: turning indicators, TTPs, incidents, vendor risk, and response lessons into shareable defensive intelligence with clear handling rules. [258, 2026]; [261, 2026].

20.3.2.2 Cyber Intelligence Fundamentals working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 20; [258, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**, with provenance and reviewability throughout.

20.3.2.3 Cyber Intelligence Fundamentals knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** fabricated alerts, public taxonomy labels, incident context, supplier evidence, and handling rules. [258, 2026]; [261, 2026].
- **Transforms:** indicator normalization, TTP mapping, confidence scoring, sharing review, and control-gap analysis.
- **Outputs:** defensive CTI packet, handling note, control implication, and incident-learning memo.
- **Failure modes:** exploit detail leakage, indicator fixation, unvetted sharing, and unsupported attribution.

20.3.2.4 Cyber Intelligence Fundamentals transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 20; [258, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**.
- **Evidence contract:** keep the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as defensive CTI packet, handling note, control implication, and incident-learning memo that another reviewer can audit.

20.3.2.5 Cyber Intelligence Fundamentals profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 20; [258, 2026].

The matched profile emphasizes turning indicators, TTPs, incidents, vendor risk, and response lessons into shareable defensive intelligence with clear handling rules. The method stack is threat-information sharing goals, indicator/TTP normalization, incident-response review, supply-chain risk assessment, and lessons learned; the local topic cluster is **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**.

20.3.3 Cyber Intelligence Fundamentals evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 20; [258, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** profile tells reviewers what evidence is strong enough for the module artifact built around **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**.

20.3.3.1 Cyber Intelligence Fundamentals guide source spine: inherited keys and local citation roles Primary guide citations: [258, 2026]; [261, 2026]; [266, 2026]; [280, 2026]; [281, 2026]; [282, 2026]; [292, 2026]; [295, 2026]; [296, 2026]; [061, 2026]; [062, 2026]; [063, 2026]; [064, 2026]; [065, 2026]; [300, 2026]; [303, 2026]; [304, 2026]; [066, 2026]; [067, 2026]; [068, 2026]; [069, 2026]; [009, 2026]; [070, 2026]; [071, 2026].

20.3.3.2 Cyber Intelligence Fundamentals verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [258, 2026]; [261, 2026].

Tier	What counts	How it is used
Source guide	[258, 2026]; [261, 2026]; [266, 2026]; [280, 2026]; [281, 2026]; [282, 2026]; [292, 2026]; [295, 2026]; [296, 2026]; [061, 2026]; [062, 2026]; [063, 2026]; [064, 2026]; [065, 2026]; [300, 2026]; [303, 2026]; [304, 2026]; [066, 2026]; [067, 2026]; [068, 2026]; [069, 2026]; [009, 2026]; [070, 2026]; [071, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 12's source-canon section, directly verified anchors for the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane include [of Standards and Technology, 2016]; [Committee, 2025]; [Committee, 2021]; [MITRE, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts** and [258, 2026]; [261, 2026], but only directly verified source URLs are encoded as citations.

20.3.3.3 Cyber Intelligence Fundamentals intelligence practice lens: evidence artifact and safety check Practice lens: **Defensive Cyber-Intelligence Lens** for **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**. [258, 2026]; [261, 2026].

Planning question: Which defensive observation, confidence level, handling rule, and control implication can be stated without teaching adversary action?

Evidence artifact: defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication.

Validation rule: verify that taxonomy labels are descriptive, indicators are contextualized, incident categories are reviewable, and outputs remain detection or assurance oriented. Applied to **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**.

Handoff contract: handoff separates observations, taxonomy labels, confidence, sharing limits, and defensive control recommendations.

Safety check: exclude exploit steps, evasion instructions, malware construction, credential misuse, phishing instructions, and live response actions.

20.3.3.4 Cyber Intelligence Fundamentals runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 20; [258, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	12.99	12.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Cyber Intelligence Fundamentals to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Bounded autonomy, procurement, incident-response, and assurance studio	12.101	12.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Cyber Intelligence Fundamentals	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Model-card, recoverability, retention, and learner-support evidence package	12.102	12.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Cyber Intelligence Fundamentals	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Cyber defensive taxonomy mapping using published labels and fabricated alerts	12.1	12.1 source title transformed into safe curriculum treatment; original: The Cyber Kill Chain (Lockheed Martin)	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Cyber defensive taxonomy mapping using published labels and fabricated alerts	12.2	12.2 source title transformed into safe curriculum treatment; original: MITRE ATT&CK Framework: Enterprise Matrix v19	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Cyber defensive taxonomy mapping using published labels and fabricated alerts	12.2.1	12.2.1 source title transformed into safe curriculum treatment; original: Reconnaissance through Resource Development	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Cyber access-and-execution taxonomy review using fabricated alerts	12.2.2	12.2.2 source title transformed into safe curriculum treatment; original: Initial Access, Execution, Persistence, Privilege Escalation	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Cyber credential-and-movement taxonomy review using fabricated alerts	12.2.3	12.2.3 source title transformed into safe curriculum treatment; original: Defense Evasion, Credential Access, Discovery, Lateral Movement	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Cyber command, data-loss, and impact taxonomy review using fabricated alerts	12.2.4	12.2.4 source title transformed into safe curriculum treatment; original: Collection, Command & Control, Exfiltration, Impact	AI/Data Accountability Lens	AI/data impact card with authority, provenance, model version, impact score, register status, human owner, and review cadence	reject automated adverse action, hidden surveillance expansion, unowned outputs, unreviewed model drift, and opaque downstream reuse
Cyber defensive taxonomy mapping using published labels and fabricated alerts	12.3	12.3 source title transformed into safe curriculum treatment; original: Unified Kill Chain: Extending Lockheed + MITRE	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Cyber defensive taxonomy mapping using published labels and fabricated alerts	12.4	12.4 source title transformed into safe curriculum treatment; original: Threat Intelligence Sharing: STIX/TAXII Standards	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Cyber defensive taxonomy mapping using published labels and fabricated alerts	12.5	12.5 source title transformed into safe curriculum treatment; original: Nation-State Cyber Espionage: Motivations and Methods	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Cyber defensive taxonomy mapping using published labels and fabricated alerts	12.6	12.6 source title transformed into safe curriculum treatment; original: Chinese State-Affiliated Hacking: APT10, APT41, Volt Typhoon	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Cyber defensive taxonomy mapping using published labels and fabricated alerts	12.7	12.7 source title transformed into safe curriculum treatment; original: Russian Cyber Operations: Sandworm, Cozy Bear, Fancy Bear	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Cyber defensive taxonomy mapping using published labels and fabricated alerts	12.8	12.8 source title transformed into safe curriculum treatment; original: Living-Off-The-Land (LOTL) Techniques in APT Operations	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings

20.3.3.5 Cyber Intelligence Fundamentals reusable subsection contract: topic rows, artifacts, and safety duties **Evidence anchor.** Section 20; [258, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Cyber defensive taxonomy mapping using published labels and fabricated alerts	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Reconnaissance through Resource Development: Cyber defensive taxonomy mapping using published labels and fabricated alerts	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Cyber access-and-execution taxonomy review using fabricated alerts	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Cyber credential-and-movement taxonomy review using fabricated alerts	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Cyber command, data-loss, and impact taxonomy review using fabricated alerts	AI/Data Accountability Lens	AI/data impact card with authority, provenance, model version, impact score, register status, human owner, and review cadence	reject automated adverse action, hidden surveillance expansion, unowned outputs, unreviewed model drift, and opaque downstream reuse
Unified Kill Chain: Cyber defensive taxonomy mapping using published labels and fabricated alerts	Defensive Cyber-Intelligence Lens	defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication	exclude exploit steps, evasion instructions, malware construction, credential misuse, phishing instructions, and live response actions
Threat Intelligence Sharing: Cyber defensive taxonomy mapping using published labels and fabricated alerts	Defensive Cyber-Intelligence Lens	defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication	exclude exploit steps, evasion instructions, malware construction, credential misuse, phishing instructions, and live response actions
Nation-State Cyber Espionage: Cyber defensive taxonomy mapping using published labels and fabricated alerts	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Chinese State-Affiliated Hacking: Cyber defensive taxonomy mapping using published labels and fabricated alerts	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Russian Cyber Operations: Cyber defensive taxonomy mapping using published labels and fabricated alerts	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Living-Off-The-Land Techniques in APT Operations: Cyber defensive taxonomy mapping using published labels and fabricated alerts	Defensive Cyber-Intelligence Lens	defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication	exclude exploit steps, evasion instructions, malware construction, credential misuse, phishing instructions, and live response actions

20.3.3.6 Cyber Intelligence Fundamentals annotated source ledger: real titles and local contribution Each source cited by this **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** module is paired below with its real title and a one-line note on what it contributes to **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**.

Source	Cited work	What it contributes	Status
[258, 2026]	OpenAPI Specification	The official OpenAPI Initiative publications page, serving as a central index for the OpenAPI Specification and related standards including the Arazzo and Overlay specifications. It provides access to multiple specification versions (2.0, 3.0, 3.1, and 3.2) and their corresponding downloadable schemas identified by release date, along with a registry of extensions, formats, media types, and other resources.	verified source-guide

Source	Cited work	What it contributes	Status
[261, 2026]	RFC 9110: HTTP Semantics	RFC 9110, the official IETF standards document defining the core semantics and architecture of HTTP, published in June 2022 and consolidating nine earlier RFCs. It establishes terminology and protocol aspects shared across HTTP versions, including methods, status codes, header fields, content negotiation, conditional and range requests, authentication, and the http and https URI schemes.	verified source-guide
[266, 2026]	PROV Overview	A W3C Working Group Note from 2013 that provides an overview and roadmap for the PROV family of specifications for representing and exchanging provenance information on the web. It defines provenance as information about the entities, activities, and people involved in producing data, used to assess quality, reliability, and trustworthiness.	verified source-guide
[280, 2026]	NIST SP 800-61 Rev. 3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management	NIST SP 800-61 Rev. 3, published April 2025, integrates incident response guidance into broader cybersecurity risk management aligned with the NIST Cybersecurity Framework 2.0, superseding the 2012 Rev. 2. The publication addresses cyber threat information sharing, incident handling and management practices, and procedures for detecting, responding to, and recovering from security incidents.	verified source-guide
[281, 2026]	Artificial Intelligence Cybersecurity Challenges	An ENISA (European Union Agency for Cybersecurity) report published December 15, 2020 mapping the cybersecurity challenges of artificial intelligence. It defines AI scope through a lifecycle approach, identifies the assets requiring protection within AI ecosystems, and develops a threat taxonomy classified across lifecycle stages and asset categories.	verified source-guide
[282, 2026]	AI Research: Security and Resilience	A NIST page on AI research focused on security and resilience, framing these as core characteristics of trustworthy AI under the NIST AI Risk Management Framework.	verified source-guide
[292, 2026]	Assessing Risks and Impacts of AI (ARIA): Pilot Evaluation Report	The ARIA 0.1 pilot evaluation report documents NIST's methodology for systematically assessing AI applications for risks and societal impacts, using a multi-layered evaluation approach across five participating organizations and seven submitted AI applications. The pilot employed three evaluation scenarios and three testing levels: model testing, red teaming, and field testing, supplemented by dialogue annotation, tester questionnaires, and structured measurement trees.	verified source-guide

Source	Cited work	What it contributes	Status
[295, 2026]	M-25-22: Driving Efficient Acquisition of Artificial Intelligence in Government	OMB Memorandum M-25-22 (April 3, 2025), Driving Efficient Acquisition of Artificial Intelligence in Government, issued under Executive Order 13960 and related directives. It provides guidance to federal agencies for acquiring effective and trustworthy AI in a timely, cost-effective manner, and rescinds and replaces earlier memorandum M-24-18.	verified source-guide
[296, 2026]	Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile	NIST AI 600-1, the Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, a cross-sectoral companion resource to the NIST AI RMF 1.0 issued pursuant to Executive Order 14110. It identifies risks that are unique to or amplified by generative AI and organizes suggested actions for managing those risks, mapped to the AI RMF functions.	verified source-guide
[061, 2026]	Cyber Kill Chain®	This Lockheed Martin webpage describes the Cyber Kill Chain framework, a methodology for identifying and preventing cyber intrusions as part of the company's Intelligence Driven Defense model. It outlines the sequence of steps an adversary must complete to achieve an objective, and is intended to help analysts understand attacker tactics and procedures.	verified source-guide
[062, 2026]	Cyber kill chain	A Wikipedia article describing the cyber kill chain, a framework adapted by Lockheed Martin from a military concept to model how cyberattacks progress through distinct phases. It outlines seven stages from reconnaissance through actions on objectives, along with defensive countermeasures organizations can apply at each stage.	verified source-guide context; do not use as primary analytic support
[063, 2026]	Enterprise Matrix - MITRE ATT&CK®	The official MITRE ATT&CK Enterprise Matrix, a curated knowledge base of adversary tactics and techniques observed in real-world intrusions. It organizes activity into fifteen sequential tactics, from reconnaissance and resource development through initial access, persistence, privilege escalation, defense evasion, credential access, lateral movement, command and control, exfiltration, and impact.	verified source-guide
[064, 2026]	MITRE ATT&CK®	MITRE ATT&CK is a globally accessible knowledge base that catalogs adversary tactics and techniques drawn from real-world observations of cyber intrusions. The framework is organized into matrices covering Enterprise, Mobile, and Industrial Control Systems environments, with tactics representing adversary objectives and techniques describing specific methods used to achieve them.	verified source-guide

Source	Cited work	What it contributes	Status
[065, 2026]	Enterprise Techniques - MITRE ATT&CK®	The Enterprise Techniques page of the MITRE ATT&CK framework, a cybersecurity knowledge base maintained by MITRE Corporation. It documents 222 enterprise techniques and 475 sub-techniques describing how adversaries achieve tactical goals across the attack lifecycle, organized by tactics such as initial access, persistence, privilege escalation, defense evasion, credential access, discovery, and impact.	verified source-guide
[300, 2026]	MITRE ATLAS	MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy.	original source-guide
[303, 2026]	Software Security in Supply Chains	An official NIST page on software supply chain security issued under Executive Order 14028, focused on the Software Bill of Materials as a formal record of software components and their supply chain. It explains the benefits of SBOMs for vulnerability identification and supply-chain transparency, recommends machine-readable formats such as SPDX, CycloneDX, and SWID, and describes foundational, sustaining, and enhancing levels of implementation.	verified source-guide
[304, 2026]	Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities	NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences.	verified source-guide
[066, 2026]	What is STIX/TAXII? - Cloudflare	A Cloudflare Learning Center explainer describing STIX and TAXII as complementary standards for cyber threat intelligence. STIX defines a structured language for representing threat information, while TAXII specifies how that information is transported and exchanged between systems. Together they form a framework that lets organizations share and consume threat intelligence in a consistent, machine-readable way to improve collective defense.	verified source-guide
[067, 2026]	Introduction to STIX	An introductory page from the OASIS CTI documentation explaining STIX (Structured Threat Information Expression), an open-source language and serialization format used to exchange cyber threat intelligence. It describes how STIX 2.1 models intelligence using 18 domain objects (such as attack patterns, malware, threat actors, and vulnerabilities) and 2 relationship objects, all represented as JSON.	verified source-guide

Source	Cited work	What it contributes	Status
[068, 2026]	OASIS Cyber Threat Intelligence (CTI) TC	The official committee page for the OASIS Cyber Threat Intelligence (CTI) Technical Committee, a standards body that develops formats for sharing cyber threat intelligence. It maintains the STIX (Structured Threat Information Expression) data model and the TAXII exchange protocol, both approved as OASIS standards in 2021, and organizes subcommittees for STIX, TAXII, and interoperability.	verified source-guide
[069, 2026]	Assessing nation-state-sponsored cyberattacks using aspects	They found that the most common cyberattacks initiated by nation-states were espionage focused.	original source-guide
[009, 2026]	"Here to stay" – Chinese state-affiliated hacking for strategic goals	A November 2023 report from MERICS (Mercator Institute for China Studies) analyzing Chinese state-affiliated cyber intrusions aimed at strategic goals. It argues that Chinese actors pursue long-term, persistent access to European technology firms and critical infrastructure for espionage rather than disruption, with targeting aligned to government priorities such as semiconductors, pharmaceuticals, and advanced manufacturing.	verified source-guide
[070, 2026]	Getting Harder to Catch Analyzing the Evolution of China's Cyber	A 2016 student security paper by Winnona DeSombre (Tufts Comp116) analyzing the evolution of China's cyber espionage campaigns against the United States. Organized in three parts, it surveys China-US relations in the cyber domain and the policy dilemmas of attribution and shared terminology, presents a case study of the APT1 hacker group linked to PLA Unit 61398, and reviews broader trends in the context of the 2015 US-China Cyber Agreement.	verified source-guide
[071, 2026]	I Led IR on Nation-State Attacks at Mandiant, FireEye & CrowdStrike	Attribution becomes harder when its open-source …	original source-guide

Where this sits. This module's overview is Section 20; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

20.3.4 Cyber Intelligence Fundamentals governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 20; [258, 2026].

20.3.5 Cyber Intelligence Fundamentals analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 12's governance-boundary section, directly verified anchors for the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane include [of Standards and Technology, 2016]; [Committee, 2025]; [Committee, 2021]; [MITRE, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Research lane: **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** for **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**. [258, 2026]; [261, 2026].
Curriculum topic spine: Cyber defensive taxonomy mapping using published labels and fabricated alerts, **MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**, **Reconnaissance through Resource Development: Cyber defensive taxonomy mapping using published labels and fabricated alerts**. **Verified anchor cluster:** [of Standards and Technology, 2016]; [Committee, 2025]; [Committee, 2021]; [MITRE, 2026b]; [Cybersecurity and Agency, 2026d]; [of Standards and Technology, 2025c]; [for Economic Co-operation and Development, 2025a].
Conceptual depth: turning indicators, TTPs, incidents, vendor risk, and response lessons into shareable defensive intelligence with clear handling rules.
Method stack: threat-information sharing goals, indicator/TTP normalization, incident-response review, supply-chain risk assessment, and lessons learned.
Composability contract: indicators, TTP mappings, affected assets, supplier evidence, response actions, and sharing constraints remain independently reusable.
Known failure modes: indicator fixation, unvetted sharing, vendor-assurance drift, weak incident scoping, and treating CTI as a feed instead of a workflow.
Defensive boundary: cyber material stays defensive and tabletop-based; it does not provide exploit, persistence, evasion, or live-response instructions.
Applied to **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**.

Anchor	Why it matters here
[of Standards and Technology, 2016]	Official guidance for establishing threat-information sharing goals, communities, distribution rules, and defensive use of indicators and TTPs. Checked as of 2026-05-21; role: curriculum_anchor.
[Committee, 2025]	OASIS CTI standard for expressing cyber threat and observable information with structured objects, relationships, sightings, and markings. Checked as of 2026-05-21; role: curriculum_anchor.
[Committee, 2021]	OASIS CTI transport standard for defensive threat-intelligence exchange channels, collections, discovery, and API contracts. Checked as of 2026-05-21; role: curriculum_anchor.
[MITRE, 2026b]	Threat-informed enterprise matrix for defensive TTP mapping, coverage analysis, detection engineering, and analytic normalization. Checked as of 2026-05-21; role: curriculum_anchor.
[Cybersecurity and Agency, 2026d]	Official catalog for prioritizing known exploited vulnerabilities as defensive triage inputs, not as exploitation instructions. Checked as of 2026-05-21; role: curriculum_anchor.
[of Standards and Technology, 2025c]	Official incident-response profile for preparation, detection, response, recovery, and continuous improvement under CSF 2.0. Checked as of 2026-05-21; role: curriculum_anchor.
[for Economic Co-operation and Development, 2025a]	OECD policy paper proposing a common AI incident reporting framework for jurisdictions and sectors, including criteria for impact and risk characterization. Checked as of 2026-05-24; role: curriculum_anchor.

20.3.5.1 Cyber Intelligence Fundamentals evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [258, 2026]; [261, 2026].

20.3.6 Cyber Intelligence Fundamentals agentic boundary: assist, approve, block, and record

Evidence anchor. Section 20; [258, 2026].
AGEINT translation is bounded by the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**.

20.3.6.1 Cyber Intelligence Fundamentals permitted defensive utility: curriculum uses and safe outputs

Evidence anchor. Section 20; [258, 2026].
The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**.

20.3.6.2 Cyber Intelligence Fundamentals excluded operational boundary: blocked actions and stop rules

Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [258, 2026]; [261, 2026] and **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

20.3.7 Cyber Intelligence Fundamentals governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 20; [258, 2026].
Governance is practiced as a gate on the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane. Learners use the **Defensive Cyber-Intelligence Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**.

20.3.7.1 Cyber Intelligence Fundamentals governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [258, 2026]; [261, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** failure modes and the **Defensive Cyber-Intelligence Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

20.3.7.2 Cyber Intelligence Fundamentals evidence package handoff: appendices, records, and reuse

Evidence anchor. Section 20; [258, 2026].
Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Defensive Cyber-Intelligence Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**.

20.3.7.3 Cyber Intelligence Fundamentals current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**. [258, 2026]; [261, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_nist_sp_800_150` for **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**?	Guide to Cyber Threat Information Sharing, NIST SP 800-150; lane `cyber_threat_intelligence`; checked 2026-05-21.	defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication; Official guidance for establishing threat-information sharing goals, communities, distribution rules, and defensive use of indicators and TTPs.
What does the module inherit from `official_oasis_stix_21` for **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**?	STIX Version 2.1; lane `cyber_threat_intelligence`; checked 2026-05-21.	defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication; OASIS CTI standard for expressing cyber threat and observable information with structured objects, relationships, sightings, and markings.
What does the module inherit from `official_oasis_taxii_21` for **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**?	TAXII Version 2.1; lane `cyber_threat_intelligence`; checked 2026-05-21.	defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication; OASIS CTI transport standard for defensive threat-intelligence exchange channels, collections, discovery, and API contracts.
What does the module inherit from `official_mitre_attack_enterprise` for **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**?	MITRE ATT&CK Enterprise Matrix; lane `cyber_threat_intelligence`; checked 2026-05-21.	defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication; Threat-informed enterprise matrix for defensive TTP mapping, coverage analysis, detection engineering, and analytic normalization.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 20; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

20.3.8 Cyber Intelligence Fundamentals assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 20; [258, 2026].

20.3.9 Cyber Intelligence Fundamentals assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 20; [258, 2026].

20.3.9.1 Cyber Intelligence Fundamentals capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**.
Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts** and [258, 2026]; [261, 2026].

20.3.9.2 Cyber Intelligence Fundamentals instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts** and [258, 2026]; [261, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

20.3.9.3 Cyber Intelligence Fundamentals assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Cyber defensive taxonomy mapping using published labels and fabricated alerts	Completed **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts	Completed **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Reconnaissance through Resource Development: Cyber defensive taxonomy mapping using published labels and fabricated alerts	Completed **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

20.3.10 Cyber Intelligence Fundamentals refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [258, 2026]; [261, 2026] and **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**.

20.3.10.1 Cyber Intelligence Fundamentals refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**. The local signals begin with [258, 2026]; [261, 2026].

20.3.10.2 Cyber Intelligence Fundamentals claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**, and the source spine for these checks begins with [258, 2026]; [261, 2026].

20.3.11 Cyber Intelligence Fundamentals reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [258, 2026]; [261, 2026].
Triangulation anchors. In module 12's review-checklist section, directly verified anchors for the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane include [of Standards and Technology, 2016]; [Committee, 2025]; [Committee, 2021]; [MITRE, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts**. [258, 2026]; [261, 2026].

- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

20.3.12 Cyber Intelligence Fundamentals learning-path links: module map, overview, and curriculum atlas

Follow the cross-links to move between **Cyber defensive taxonomy mapping using published labels and fabricated alerts; MITRE ATT&CK Framework: Cyber defensive taxonomy mapping using published labels and fabricated alerts** and the rest of the curriculum without losing the source spine: orientation first, then the parent unit, then the modules on either side. Primary sources: [258, 2026]; [261, 2026].
Section 2, Section 19, Section 21

21 Advanced Persistent Threats (APTs)

21.0.1 Advanced Persistent Threats (APTs) figures and course links: visual evidence, source flow, and navigation

The module uses Figure 55 and Figure 52 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.

Navigation links: Section 2, Section 19, Section 20, Section 22.

This module teaches the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane through a bounded, source-backed coursebook chapter. [237, 2026]; [258, 2026].

21.1 Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense frame for Advanced Persistent Threats (APTs): source context, topic focus, and reader task

Evidence anchor. Section 21; [237, 2026].

21.1.1 Advanced Persistent Threats (APTs) orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 21; [237, 2026].

21.1.2 Advanced Persistent Threats (APTs) conceptual primer: source context, core model, and reader task

This chapter teaches cyber threat intelligence as defensive normalization: incidents, indicators, TTPs, vendor risks, and sharing rules become useful only when scoped and validated. The chapter uses **Defensive Cyber-Intelligence Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**.

The central distinction is to separate defensive mapping and incident learning from exploit, persistence, or evasion instruction. Core topics include **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis; Nation-State vs. Ideological Actor Attack Patterns**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.

Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [of Standards and Technology, 2016]; [Committee, 2025]; [Committee, 2021]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [237, 2026]; [258, 2026].

Learners move from vocabulary and the **Defensive Cyber-Intelligence Lens** distinction through topic lessons on **APT Definitions, Lifecycle, and Attribution** with evidence and misconception checks, then assemble a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** with safety and rights gates.

21.1.3 Advanced Persistent Threats (APTs) learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 21; [237, 2026].

- Connect **APT Definitions, Lifecycle, and Attribution and APT Risk Propagation Models: ATT&CK-Based Analysis** to **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate defensive mapping and incident learning from exploit, persistence, or evasion instruction; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as indicator fixation, unvetted sharing, vendor-assurance drift, weak incident scoping, and treating CTI as a feed instead of a workflow, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: cyber material stays defensive and tabletop-based; it does not provide exploit, persistence, evasion, or live-response instructions.

21.1.4 Advanced Persistent Threats (APTs) core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 21; [237, 2026].

Term	Working definition
Indicator	an observable signal that may support defensive detection or investigation
TTP	a tactic, technique, or procedure used for structured defensive mapping
Sighting	a bounded observation of a possible indicator in a given context
Handling rule	a sharing, marking, or retention limit for threat information
Lessons learned	the post-incident evidence that changes controls or playbooks
APT Definitions, Lifecycle, and Attribution	Key terms: APT, Definitions, Lifecycle.
APT Risk Propagation Models: ATT&CK-Based…	Key terms: APT, Risk, Propagation.

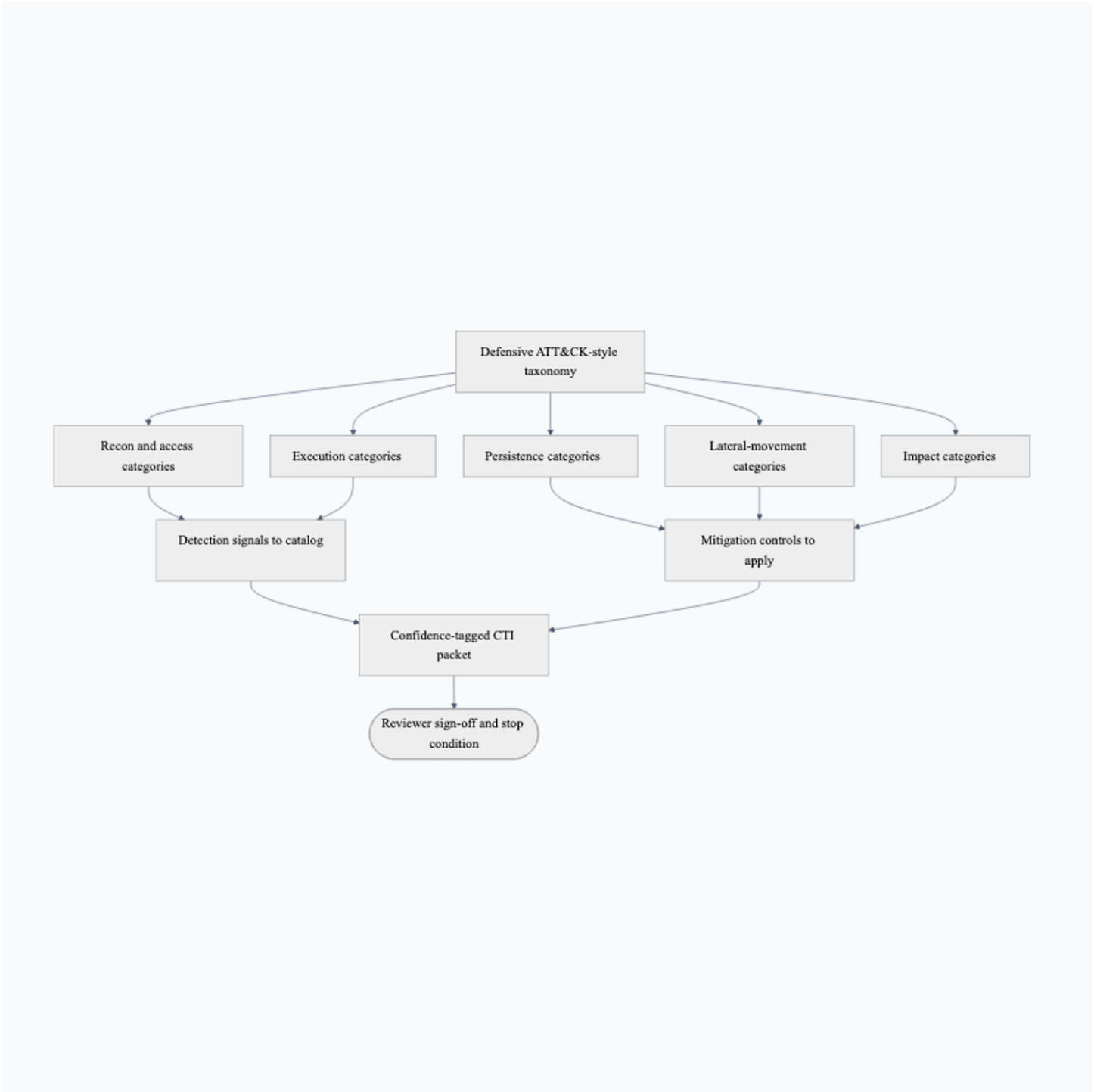


Figure 55: This diagram organizes the ATT&CK-style adversary tactic categories purely as a defensive taxonomy, mapping each phase to the detection signals and mitigation controls a defender catalogs, never to attack instructions. It is anchored to the technical intelligence and cyber operations / advanced persistent threats apts section; use it to inspect Defensive ATT&CK-style taxonomy, Recon and access categories, Execution categories, and Persistence categories while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

21.2 Defensive Cyber-Intelligence Lens path for Advanced Persistent Threats (APTs): lesson cluster, safe artifact, and review

Evidence anchor. Section 21; [237, 2026].

21.2.1 Advanced Persistent Threats (APTs) practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 21; [237, 2026].

21.2.2 Advanced Persistent Threats (APTs) topic lessons: source-backed concepts and transfer tasks

This module builds cyber threat intelligence as defensive normalization: incidents, indicators, TTPs, vendor risks, and sharing rules become useful only when scoped and validated. The sequence opens with **APT Definitions, Lifecycle, and Attribution**, **APT Risk Propagation Models: ATT&CK-Based Analysis**, **Nation-State vs. Ideological Actor Attack Patterns** and applies the **Defensive Cyber-Intelligence Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 52; module overview Section 21; curriculum atlas Section 2.

Triangulation anchors. In module 13's topic-lessons section, directly verified anchors for the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane include [of Standards and Technology, 2016]; [Committee, 2025]; [Committee, 2021]; [MITRE, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

21.2.2.1 Lesson 1: APT Definitions, Lifecycle, and Attribution **Concept. APT Definitions, Lifecycle, and Attribution** studies APT reporting as attribution and confidence literacy: technical similarity, context, caveats, and geopolitical inference stay separate.

Why it matters. Analysts use **APT Definitions, Lifecycle, and Attribution** to separate defensive mapping and incident learning from exploit, persistence, or evasion instruction. A defensible treatment names the judgment it enables for defensive CTI normalization and tabletop incident learning review, the proof limit that indicator fixation would otherwise hide, and the reviewer accountable for challenge.

Source support. APT Definitions, Lifecycle, and Attribution rests on [072, 2026]. The lead source's own note reads: The Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework introduced. Use it for the claim that **APT Definitions, Lifecycle, and Attribution** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. For **APT Definitions, Lifecycle, and Attribution**, reason from the sources cited in this row. [072, 2026] The Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework introduced. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **APT Definitions, Lifecycle, and Attribution**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this defensive CTI normalization and tabletop incident learning topic. The artifact must name the source descriptor, the bounded claim about **APT Definitions Lifecycle and Attribution**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape this subject work as a **defensive CTI evidence packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that APT Definitions, Lifecycle, and Attribution can be used while ignoring the rule to separate defensive mapping and incident learning from exploit, persistence, or evasion instruction.

Transfer task. Transfer **APT Definitions, Lifecycle, and Attribution** to a second module by preserving defensive CTI normalization and tabletop incident learning, changing the source evidence, and naming a new reviewer.

21.2.2.2 Lesson 2: APT Risk Propagation Models: ATT&CK-Based Analysis **Concept. APT Risk Propagation Models: ATT&CK-Based Analysis** studies APT reporting as attribution and confidence literacy: technical similarity, context, caveats, and geopolitical inference stay separate.

Why it matters. APT Risk Propagation Models matters in the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane because defensive CTI normalization and tabletop incident learning evidence must stay separate from judgment; indicator fixation is a common failure.

Source support. APT Risk Propagation Models: ATT&CK-Based Analysis rests on [072, 2026]. The most specific cited work observes: The Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework introduced. Use it for the working definition that **APT Risk Propagation Models: ATT&CK-Based Analysis** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. Ground **APT Risk Propagation Models** in the evidence the row cites. [072, 2026] The Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework introduced. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **APT Risk Propagation Models**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this defensive CTI normalization and tabletop incident learning topic. The artifact must name the source descriptor, the bounded claim about **APT Risk Propagation Models**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **APT Risk Propagation Models** work as a **defensive CTI evidence packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that APT Risk Propagation Models: ATT&CK-Based Analysis is optional whenever separate defensive mapping and incident learning from exploit, persistence, or evasion instruction feels inconvenient.

Transfer task. Transfer **APT Risk Propagation Models** to a second module by preserving defensive CTI normalization and tabletop incident learning, changing the source evidence, and naming a new reviewer.

21.2.2.3 Lesson 3: Nation-State vs. Ideological Actor Attack Patterns **Concept. Nation-State vs. Ideological Actor Attack Patterns** applies Nation, State, Ideological within Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense: learners use separate defensive mapping and incident learning from exploit, persistence, or evasion instruction and defensive CTI normalization and tabletop incident learning evidence before any judgment moves forward.

Why it matters. Analysts use **Nation-State vs. Ideological Actor Attack Patterns** to separate defensive mapping and incident learning from exploit, persistence, or evasion instruction. A defensible treatment names the judgment it enables for defensive CTI normalization and tabletop incident learning review, the proof limit that indicator fixation would otherwise hide, and the reviewer accountable for challenge.

Source support. Nation-State vs. Ideological Actor Attack Patterns rests on [069, 2026]. Its anchor reference records: They found that the most common cyberattacks initiated by nation-states were espionage focused. Use it for pinning down the scope of **Nation-State vs. Ideological Actor Attack Patterns**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. For **Nation-State vs. Ideological Actor Attack Patterns**, reason from the sources cited in this row. [069, 2026] They found that the most common cyberattacks initiated by nation-states were espionage focused. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Nation-State vs. Ideological Actor Attack Patterns**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this defensive CTI normalization and tabletop incident learning topic. The artifact must name the source descriptor, the bounded claim about **Nation-State vs Ideological Actor Attack**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape this subject work as a **defensive CTI evidence packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that Nation-State vs. Ideological Actor Attack Patterns establishes intent without reviewing alternative explanations.

Transfer task. Transfer **Nation-State vs. Ideological Actor Attack Patterns** to a second module by preserving defensive CTI normalization and tabletop incident learning, changing the source evidence, and naming a new reviewer.

21.2.2.4 Lesson 4: Cyber infrastructure-abuse indicator review using fabricated records

Concept. Cyber infrastructure-abuse indicator review using fabricated records studies APT reporting as attribution and confidence literacy: technical similarity, context, caveats, and geopolitical inference stay separate.

Why it matters. Cyber infrastructure-abuse indicator review matters in the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane because defensive CTI normalization and tabletop incident learning evidence must stay separate from judgment; treating defensive taxonomy labels as an action sequence is a common failure.

Source support. Cyber infrastructure-abuse indicator review using fabricated records rests on [300, 2026], [303, 2026], and [304, 2026]. The most specific cited work observes: It explains the benefits of SBOMs for vulnerability identification and supply-chain transparency, recommends machine-readable formats such as SPDX, CycloneDX, and SWID, and describes foundational, sustaining, and enhancing levels of implementation. Use them for the working definition that **Cyber infrastructure-abuse indicator review using fabricated records** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. Read **Cyber infrastructure-abuse indicator review** against the works cited for this row. [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. [303, 2026] An official NIST page on software supply chain security issued under Executive Order 14028, focused on the Software Bill of Materials as a formal record of software components and their supply chain. It explains the benefits of SBOMs for vulnerability identification and supply-chain transparency, recommends machine-readable formats such as SPDX, CycloneDX, and SWID, and describes foundational, sustaining, and enhancing levels of implementation. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Cyber infrastructure-abuse indicator review**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this defensive CTI normalization and tabletop incident learning topic. The artifact must map the indicator descriptor, the bounded claim about **Cyber infrastructure-abuse indicator review using**, the taxonomy caveat, the confidence note, the no-action boundary, and the reviewer who validates the labeling. Shape **Cyber infrastructure-abuse indicator review** work as a **defensive CTI evidence packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Cyber infrastructure-abuse indicator review**: that a defensive taxonomy label is an action sequence rather than a vocabulary for describing and detecting behavior.

Transfer task. Apply this module's safe boundary for **Cyber infrastructure-abuse indicator review** to another artifact while keeping defensive CTI normalization and tabletop incident learning and reviewer ownership explicit.

21.2.2.5 Lesson 5: Incident Response on Nation-State Intrusions: Mandiant Methodology

Concept. Incident Response on Nation-State Intrusions: Mandiant Methodology maps incident phases to evidence preservation, stakeholder notification, learning loops, and defensive control updates.

Why it matters. Incident Response on Nation-State Intrusions connects classroom vocabulary to Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Incident Response on Nation-State Intrusions: Mandiant Methodology rests on [071, 2026]. The closest source to this row notes: Attribution becomes harder when its open-source … Use it for the working definition that **Incident Response on Nation-State Intrusions: Mandiant Methodology** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. Read **Incident Response on Nation-State Intrusions** against the works cited for this row. [071, 2026] Attribution becomes harder when its open-source … From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Incident Response on Nation-State Intrusions**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this defensive CTI normalization and tabletop incident learning topic. The artifact must name the source descriptor, the bounded claim about **Incident Response on Nation-State Intrusions**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Incident Response on Nation-State Intrusions** work as a **defensive CTI evidence packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that Incident Response on Nation-State Intrusions: Mandiant Methodology can be used while ignoring the rule to separate defensive mapping and incident learning from exploit, persistence, or evasion instruction.

Transfer task. Transfer **Incident Response on Nation-State Intrusions** to a second module by preserving defensive CTI normalization and tabletop incident learning, changing the source evidence, and naming a new reviewer.

21.2.2.6 Lesson 6: Threat Hunting Against APT Actors

Concept. Threat Hunting Against APT Actors studies APT reporting as attribution and confidence literacy: technical similarity, context, caveats, and geopolitical inference stay separate.

Why it matters. Threat Hunting Against APT Actors matters in the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane because defensive CTI normalization and tabletop incident learning evidence must stay separate from judgment; indicator fixation is a common failure.

Source support. Threat Hunting Against APT Actors rests on [300, 2026], [303, 2026], and [304, 2026]. The closest source to this row notes: It explains the benefits of SBOMs for vulnerability identification and supply-chain transparency, recommends machine-readable formats such as SPDX, CycloneDX, and SWID, and describes foundational, sustaining, and enhancing levels of implementation. Use them for fixing what **Threat Hunting Against APT Actors** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. Ground **Threat Hunting Against APT Actors** in the evidence the row cites. [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. [303, 2026] An official NIST page on software supply chain security issued under Executive Order 14028, focused on the Software Bill of Materials as a formal record of software components and their supply chain. It explains the benefits of SBOMs for vulnerability identification and supply-chain transparency, recommends machine-readable formats such as SPDX, CycloneDX, and SWID, and describes foundational, sustaining, and enhancing levels of implementation. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating

security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. Build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this defensive CTI normalization and tabletop incident learning topic. The artifact must name the source descriptor, the bounded claim about **Threat Hunting Against APT Actors**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape this subject work as a **defensive CTI evidence packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that Threat Hunting Against APT Actors is optional whenever separate defensive mapping and incident learning from exploit, persistence, or evasion instruction feels inconvenient.

Transfer task. Transfer **Threat Hunting Against APT Actors** to a second module by preserving defensive CTI normalization and tabletop incident learning, changing the source evidence, and naming a new reviewer.

21.2.2.7 Lesson 7: APT Attribution: Technical Indicators vs. Geopolitical Context

Concept. APT Attribution: Technical Indicators vs. Geopolitical Context studies APT reporting as attribution and confidence literacy: technical similarity, context, caveats, and geopolitical inference stay separate.

Why it matters. APT Attribution: Technical Indicators vs. Geopolitical Context connects classroom vocabulary to Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. APT Attribution: Technical Indicators vs. Geopolitical Context rests on [309, 2026], [310, 2026], and [300, 2026]. Its anchor reference records: The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. Use them for fixing what **APT Attribution: Technical Indicators vs. Geopolitical Context** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. Ground **APT Attribution: Technical Indicators vs. Geopolitical Context** in the evidence the row cites. [309, 2026] An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection. [310, 2026] The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **APT Attribution**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this defensive CTI normalization and tabletop incident learning topic. The artifact must name the source descriptor, the bounded claim about **APT Attribution**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **APT Attribution: Technical Indicators vs. Geopolitical Context** work as a **defensive CTI evidence packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that APT Attribution: Technical Indicators vs. Geopolitical Context establishes intent without reviewing alternative explanations.

Transfer task. Transfer **APT Attribution: Technical Indicators vs. Geopolitical Context** to a second module by preserving defensive CTI normalization and tabletop incident learning, changing the source evidence, and naming a new reviewer.

21.2.3 Advanced Persistent Threats (APTs) worked safe example: synthetic inputs, evidence, and review

Worked example: a sample campus SOC reviews fabricated alert records after a tabletop incident. [237, 2026]; [258, 2026].

Triangulation anchors. In module 13's worked-example section, directly verified anchors for the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane include [of Standards and Technology, 2016]; [Committee, 2025]; [Committee, 2021]; [MITRE, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **defensive cyber intelligence normalization**. Learners use a **defensive CTI evidence packet** and keep this boundary visible: No exploit, persistence, evasion, scanning, or production response instructions.

Frame. The classroom question centers on **APT Definitions, Lifecycle, and Attribution**. Excluded actions stay explicit, and the **Defensive Cyber-Intelligence Lens** planning question is: Which defensive observation, confidence level, handling rule, and control implication can be stated without teaching adversary action?

Inputs. For the **APT Definitions, Lifecycle, and Attribution** scenario, use toy alerts, synthetic asset names, public ATT&CK technique descriptions, and a sharing-policy card. The Defensive Cyber-Intelligence Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **APT Definitions, Lifecycle, and Attribution**, students normalize indicators, map TTPs defensively, rate confidence, mark sharing limits, and record lessons learned. Pause whenever an inference about APT Definitions, Lifecycle, and Attribution appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **APT Definitions, Lifecycle, and Attribution** classroom scenario; unit artifact = defensive CTI evidence packet; evidence = allowed inputs; method = defensive CTI normalization and tabletop incident learning; output = a CTI packet with indicators, TTP mapping, confidence, handling rule, and remediation owner; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **APT Definitions, Lifecycle, and Attribution** as "Defensive Cyber-Intelligence Lens confirms it" is not enough. The revision ties the claim to defensive CTI normalization and tabletop incident learning, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **APT Definitions, Lifecycle, and Attribution** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

21.2.4 Advanced Persistent Threats (APTs) practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Defensive Cyber-Intelligence Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**.

Triangulation anchors. In module 13's practice-sequence section, directly verified anchors for the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane include [of Standards and Technology, 2016]; [Committee, 2025]; [Committee, 2021]; [MITRE, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare APT Definitions, Lifecycle, and Attribution, APT Risk Propagation Models: ATT&CK-Based Analysis, Nation-State vs. Ideological Actor Attack Patterns; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane.
2. Frame	Answer the lens question: Which defensive observation, confidence level, handling rule, and control implication can be stated without teaching adversary action?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for APT Definitions, Lifecycle, and Attribution: defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the defensive CTI evidence packet fields for APT Definitions, Lifecycle, and Attribution.	Unit profile note.	Evidence artifacts include indicator context, TTP mapping.
4. Challenge	Test the misconception that APT Definitions, Lifecycle, and Attribution can be used while ignoring the rule to separate defensive mapping and incident learning from exploit, persistence, or evasion instruction.	Failure-mode note.	The artifact applies the key distinction: separate defensive mapping and incident learning from exploit, persistence, or evasion instruction.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

21.2.4.1 Advanced Persistent Threats (APTs) instructor notes: source reasoning, review points, and studio focus Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**. [237, 2026]; [258, 2026].

21.2.4.2 Advanced Persistent Threats (APTs) extension exercise: peer validation and refresh trigger review **Evidence anchor.** Section 21; [237, 2026].
Have learners swap artifacts and apply the **Defensive Cyber-Intelligence Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**.

21.2.5 Advanced Persistent Threats (APTs) knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 21; [237, 2026].

1. Explain how **APT Definitions, Lifecycle, and Attribution** is defined here; name the source descriptor that supports the definition.
2. Contrast **APT Definitions, Lifecycle, and Attribution** with **APT Risk Propagation Models: ATT&CK-Based Analysis** using the **Defensive Cyber-Intelligence Lens** artifact fields.
3. Identify one failure mode from the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which indicator is useful only after context and confidence are added?
5. Correct this misconception: that APT Definitions, Lifecycle, and Attribution can be used while ignoring the rule to separate defensive mapping and incident learning from exploit, persistence, or evasion instruction.

21.2.5.1 Advanced Persistent Threats (APTs) answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **APT Definitions, Lifecycle, and Attribution** without source evidence, uncertainty, or a safe transfer task.

21.3 Advanced Persistent Threats (APTs) assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 21; [237, 2026].

21.3.1 Advanced Persistent Threats (APTs) evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 21; [237, 2026].

21.3.2 Advanced Persistent Threats (APTs) transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 21; [237, 2026].

21.3.2.1 Advanced Persistent Threats (APTs) lineage and source tradition: profile, concepts, and first anchors This sits in the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lineage: turning indicators, TTPs, incidents, vendor risk, and response lessons into shareable defensive intelligence with clear handling rules. [237, 2026]; [258, 2026].

21.3.2.2 Advanced Persistent Threats (APTs) working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 21; [237, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**, with provenance and reviewability throughout.

21.3.2.3 Advanced Persistent Threats (APTs) knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** fabricated alerts, public taxonomy labels, incident context, supplier evidence, and handling rules. [237, 2026]; [258, 2026].
- **Transforms:** indicator normalization, TTP mapping, confidence scoring, sharing review, and control-gap analysis.
- **Outputs:** defensive CTI packet, handling note, control implication, and incident-learning memo.
- **Failure modes:** exploit detail leakage, indicator fixation, unvetted sharing, and unsupported attribution.

21.3.2.4 Advanced Persistent Threats (APTs) transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 21; [237, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**.
- **Evidence contract:** keep the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as defensive CTI packet, handling note, control implication, and incident-learning memo that another reviewer can audit.

21.3.2.5 Advanced Persistent Threats (APTs) profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 21; [237, 2026].

The matched profile emphasizes turning indicators, TTPs, incidents, vendor risk, and response lessons into shareable defensive intelligence with clear handling rules. The method stack is threat-information sharing goals, indicator/TTP normalization, incident-response review, supply-chain risk assessment, and lessons learned; the local topic cluster is **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**.

21.3.3 Advanced Persistent Threats (APTs) evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 21; [237, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** profile tells reviewers what evidence is strong enough for the module artifact built around **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**.

21.3.3.1 Advanced Persistent Threats (APTs) guide source spine: inherited keys and local citation roles Primary guide citations: [237, 2026]; [258, 2026]; [261, 2026]; [273, 2026]; [276, 2026]; [285, 2026]; [286, 2026]; [290, 2026]; [294, 2026]; [072, 2026]; [069, 2026]; [071, 2026]; [300, 2026]; [303, 2026]; [304, 2026]; [309, 2026]; [310, 2026].

21.3.3.2 Advanced Persistent Threats (APTs) verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [237, 2026]; [258, 2026].

Tier	What counts	How it is used
Source guide	[237, 2026]; [258, 2026]; [261, 2026]; [273, 2026]; [276, 2026]; [285, 2026]; [286, 2026]; [290, 2026]; [294, 2026]; [072, 2026]; [069, 2026]; [071, 2026]; [300, 2026]; [303, 2026]; [304, 2026]; [309, 2026]; [310, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 13's source-canon section, directly verified anchors for the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane include [of Standards and Technology, 2016]; [Committee, 2025]; [Committee, 2021]; [MITRE, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis** and [237, 2026]; [258, 2026], but only directly verified source URLs are encoded as citations.

21.3.3.3 Advanced Persistent Threats (APTs) intelligence practice lens: evidence artifact and safety check Practice lens: **Defensive Cyber-Intelligence Lens** for **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**. [237, 2026]; [258, 2026].

Planning question: Which defensive observation, confidence level, handling rule, and control implication can be stated without teaching adversary action?

Evidence artifact: defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication.

Validation rule: verify that taxonomy labels are descriptive, indicators are contextualized, incident categories are reviewable, and outputs remain detection or assurance oriented. Applied to **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**.

Handoff contract: handoff separates observations, taxonomy labels, confidence, sharing limits, and defensive control recommendations.

Safety check: exclude exploit steps, evasion instructions, malware construction, credential misuse, phishing instructions, and live response actions.

21.3.3.4 Advanced Persistent Threats (APTs) runtime-to-reader map: generated sections and verifier surfaces **Evidence anchor.** Section 21; [237, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	13.99	13.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Advanced Persistent Threats (APTs) to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Bounded autonomy, procurement, incident-response, and assurance studio	13.101	13.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Advanced Persistent Threats (APTs)	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Model-card, recoverability, retention, and learner-support evidence package	13.102	13.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Advanced Persistent Threats (APTs)	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
APT Definitions, Lifecycle, and Attribution	13.1	13.1 APT Definitions, Lifecycle, and Attribution	Defensive Cyber-Intelligence Lens	defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication	exclude exploit steps, evasion instructions, malware construction, credential misuse, phishing instructions, and live response actions
APT Risk Propagation Models: ATT&CK-Based Analysis	13.2	13.2 APT Risk Propagation Models: ATT&CK-Based Analysis	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Nation-State vs. Ideological Actor Attack Patterns	13.3	13.3 Nation-State vs. Ideological Actor Attack Patterns	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Cyber infrastructure-abuse indicator review using fabricated records	13.4	13.4 source title transformed into safe curriculum treatment; original: APT Infrastructure: C2 Frameworks, Domain Fronting, Bulletproof Hosting	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Incident Response on Nation-State Intrusions: Mandiant Methodology	13.5	13.5 Incident Response on Nation-State Intrusions: Mandiant Methodology	Defensive Cyber-Intelligence Lens	defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication	exclude exploit steps, evasion instructions, malware construction, credential misuse, phishing instructions, and live response actions
Threat Hunting Against APT Actors	13.6	13.6 Threat Hunting Against APT Actors	Defensive Cyber-Intelligence Lens	defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication	exclude exploit steps, evasion instructions, malware construction, credential misuse, phishing instructions, and live response actions
APT Attribution: Technical Indicators vs. Geopolitical Context	13.7	13.7 APT Attribution: Technical Indicators vs. Geopolitical Context	Defensive Cyber-Intelligence Lens	defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication	exclude exploit steps, evasion instructions, malware construction, credential misuse, phishing instructions, and live response actions

21.3.3.5 Advanced Persistent Threats (APTs) reusable subsection contract: topic rows, artifacts, and safety duties Evidence anchor. Section 21; [237, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
APT Definitions, Lifecycle, and Attribution	Defensive Cyber-Intelligence Lens	defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication	exclude exploit steps, evasion instructions, malware construction, credential misuse, phishing instructions, and live response actions
APT Risk Propagation Models: ATT&CK-Based Analysis	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Nation-State vs. Ideological Actor Attack Patterns	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Cyber infrastructure-abuse indicator review using fabricated records	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Incident Response on Nation-State Intrusions: Mandiant Methodology	Defensive Cyber-Intelligence Lens	defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication	exclude exploit steps, evasion instructions, malware construction, credential misuse, phishing instructions, and live response actions
Threat Hunting Against APT Actors	Defensive Cyber-Intelligence Lens	defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication	exclude exploit steps, evasion instructions, malware construction, credential misuse, phishing instructions, and live response actions

Lesson topic	Practice lens	Evidence artifact	Safety check
APT Attribution: Technical Indicators vs. Geopolitical Context	Defensive Cyber-Intelligence Lens	defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication	exclude exploit steps, evasion instructions, malware construction, credential misuse, phishing instructions, and live response actions

21.3.3.6 Advanced Persistent Threats (APTs) annotated source ledger: real titles and local contribution Each source cited by this **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** module is paired below with its real title and a one-line note on what it contributes to **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**.

Source	Cited work	What it contributes	Status
[237, 2026]	Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities	Official GAO AI accountability framework.	original source-guide
[258, 2026]	OpenAPI Specification	The official OpenAPI Initiative publications page, serving as a central index for the OpenAPI Specification and related standards including the Arazzo and Overlay specifications. It provides access to multiple specification versions (2.0, 3.0, 3.1, and 3.2) and their corresponding downloadable schemas identified by release date, along with a registry of extensions, formats, media types, and other resources.	verified source-guide
[261, 2026]	RFC 9110: HTTP Semantics	RFC 9110, the official IETF standards document defining the core semantics and architecture of HTTP, published in June 2022 and consolidating nine earlier RFCs. It establishes terminology and protocol aspects shared across HTTP versions, including methods, status codes, header fields, content negotiation, conditional and range requests, authentication, and the http and https URI schemes.	verified source-guide
[273, 2026]	WCAG 2 Overview	The W3C Web Accessibility Initiative overview of the Web Content Accessibility Guidelines (WCAG), an international standard for making web content accessible to people with disabilities. It explains that WCAG is organized around four principles (perceivable, operable, understandable, robust) with testable success criteria at three conformance levels (A, AA, AAA), and covers versions 2.0, 2.1, and 2.2.	verified source-guide
[276, 2026]	What is a Data Protection Impact Assessment and When Is This Mandatory?	A European Data Protection Board FAQ page, part of its data protection guide for small businesses, explaining Data Protection Impact Assessments (DPIAs) and when they are mandatory. It describes a DPIA as a written assessment of the impact of a planned processing operation, required when processing poses high risks to individuals' rights.	verified source-guide
[285, 2026]	NIST AI Resource Center	The NIST AI Resource Center (AIRC), a government platform supporting implementation of the NIST AI Risk Management Framework, a voluntary framework for managing AI risk. It provides the core framework along with a playbook of practical actions, profiles tailored to specific sectors and technologies, use cases, and crosswalks linking the framework to other governance structures.	verified source-guide

Source	Cited work	What it contributes	Status
[286, 2026]	Model Cards for Model Reporting	The arXiv abstract for "Model Cards for Model Reporting" (2018) by Mitchell, Wu, Zaldivar, and colleagues, which introduces a framework for transparent documentation of machine learning models. Model cards are short accompanying documents that report a model's benchmarked performance across varied conditions, including different cultural, demographic, and phenotypic groups, along with intended use, evaluation methodology, and deployment considerations.	verified source-guide
[290, 2026]	NIST SP 800-218A: Secure Software Development Practices for Generative AI and Dual-Use Foundation Models	NIST Special Publication 800-218A (July 2024), which augments the Secure Software Development Framework with practices specific to AI model development across the software lifecycle. Produced in response to Executive Order 14110, it addresses AI model producers, developers building on those models, and acquirers of AI systems, and is designed to be used alongside NIST SP 800-218.	verified source-guide
[294, 2026]	M-25-21: Accelerating Federal Use of AI through Innovation, Governance, and Public Trust	An April 2025 Office of Management and Budget memorandum (M-25-21) directing executive branch agencies on federal use of artificial intelligence. Issued under Executive Order 14179, it instructs agencies to accelerate adoption of AI to improve public services and government efficiency while maintaining safeguards for civil rights, civil liberties, and privacy.	verified source-guide
[072, 2026]	ATT&CK-based Advanced Persistent Threat attacks risk propagation	The Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework introduced.	original source-guide
[069, 2026]	Assessing nation-state-sponsored cyberattacks using aspects	They found that the most common cyberattacks initiated by nation-states were espionage focused.	original source-guide
[071, 2026]	I Led IR on Nation-State Attacks at Mandiant, FireEye & CrowdStrike	Attribution becomes harder when its open-source …	original source-guide
[300, 2026]	MITRE ATLAS	MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy.	original source-guide
[303, 2026]	Software Security in Supply Chains	An official NIST page on software supply chain security issued under Executive Order 14028, focused on the Software Bill of Materials as a formal record of software components and their supply chain. It explains the benefits of SBOMs for vulnerability identification and supply-chain transparency, recommends machine-readable formats such as SPDX, CycloneDX, and SWID, and describes foundational, sustaining, and enhancing levels of implementation.	verified source-guide

Source	Cited work	What it contributes	Status
[304, 2026]	Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities	NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences.	verified source-guide
[309, 2026]	STIX Version 2.1	An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection.	verified source-guide
[310, 2026]	TAXII Version 2.1	The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe).	verified source-guide

Where this sits. This module's overview is Section 21; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

21.3.4 Advanced Persistent Threats (APTs) governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 21; [237, 2026].

21.3.5 Advanced Persistent Threats (APTs) analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 13's governance-boundary section, directly verified anchors for the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane include [of Standards and Technology, 2016]; [Committee, 2025]; [Committee, 2021]; [MITRE, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Research lane: **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** for **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**. [237, 2026]; [258, 2026].
Curriculum topic spine: APT Definitions, Lifecycle, and Attribution, **APT Risk Propagation Models: ATT&CK-Based Analysis**, **Nation-State vs. Ideological Actor Attack Patterns**. **Verified anchor cluster:** [of Standards and Technology, 2016]; [Committee, 2025]; [Committee, 2021]; [MITRE, 2026b]; [Cybersecurity and Agency, 2026d]; [of Standards and Technology, 2025c]; [for Economic Co-operation and Development, 2025a].
Conceptual depth: turning indicators, TTPs, incidents, vendor risk, and response lessons into shareable defensive intelligence with clear handling rules.
Method stack: threat-information sharing goals, indicator/TTP normalization, incident-response review, supply-chain risk assessment, and lessons learned.
Composability contract: indicators, TTP mappings, affected assets, supplier evidence, response actions, and sharing constraints remain independently reusable.
Known failure modes: indicator fixation, unvetted sharing, vendor-assurance drift, weak incident scoping, and treating CTI as a feed instead of a workflow.
Defensive boundary: cyber material stays defensive and tabletop-based; it does not provide exploit, persistence, evasion, or live-response instructions.
Applied to **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**.

Anchor	Why it matters here
[of Standards and Technology, 2016]	Official guidance for establishing threat-information sharing goals, communities, distribution rules, and defensive use of indicators and TTPs. Checked as of 2026-05-21; role: curriculum_anchor.
[Committee, 2025]	OASIS CTI standard for expressing cyber threat and observable information with structured objects, relationships, sightings, and markings. Checked as of 2026-05-21; role: curriculum_anchor.
[Committee, 2021]	OASIS CTI transport standard for defensive threat-intelligence exchange channels, collections, discovery, and API contracts. Checked as of 2026-05-21; role: curriculum_anchor.
[MITRE, 2026b]	Threat-informed enterprise matrix for defensive TTP mapping, coverage analysis, detection engineering, and analytic normalization. Checked as of 2026-05-21; role: curriculum_anchor.
[Cybersecurity and Agency, 2026d]	Official catalog for prioritizing known exploited vulnerabilities as defensive triage inputs, not as exploitation instructions. Checked as of 2026-05-21; role: curriculum_anchor.
[of Standards and Technology, 2025c]	Official incident-response profile for preparation, detection, response, recovery, and continuous improvement under CSF 2.0. Checked as of 2026-05-21; role: curriculum_anchor.
[for Economic Co-operation and Development, 2025a]	OECD policy paper proposing a common AI incident reporting framework for jurisdictions and sectors, including criteria for impact and risk characterization. Checked as of 2026-05-24; role: curriculum_anchor.

21.3.5.1 Advanced Persistent Threats (APTs) evidence standard and citation floor: source families and discovery limits Official guidance supplies governance, safety, and legal constraints for the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [237, 2026]; [258, 2026].

21.3.6 Advanced Persistent Threats (APTs) agentic boundary: assist, approve, block, and record

Evidence anchor. Section 21; [237, 2026].
AGEINT translation is bounded by the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**.

21.3.6.1 Advanced Persistent Threats (APTs) permitted defensive utility: curriculum uses and safe outputs **Evidence anchor.** Section 21; [237, 2026].
The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**.

21.3.6.2 Advanced Persistent Threats (APTs) excluded operational boundary: blocked actions and stop rules Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [237, 2026]; [258, 2026] and **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

21.3.7 Advanced Persistent Threats (APTs) governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 21; [237, 2026].
Governance is practiced as a gate on the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane. Learners use the **Defensive Cyber-Intelligence Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues

remain, and when an agent-assisted artifact must stop for human review while using **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**.

21.3.7.1 Advanced Persistent Threats (APTs) governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [237, 2026]; [258, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** failure modes and the **Defensive Cyber-Intelligence Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

21.3.7.2 Advanced Persistent Threats (APTs) evidence package handoff: appendices, records, and reuse

Evidence anchor. Section 21; [237, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Defensive Cyber-Intelligence Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**.

21.3.7.3 Advanced Persistent Threats (APTs) current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**. [237, 2026]; [258, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_nist_sp_800_150` for **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**?	Guide to Cyber Threat Information Sharing, NIST SP 800-150; lane `cyber_threat_intelligence`; checked 2026-05-21.	defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication; Official guidance for establishing threat-information sharing goals, communities, distribution rules, and defensive use of indicators and TTPs.
What does the module inherit from `official_oasis_stix_21` for **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**?	STIX Version 2.1; lane `cyber_threat_intelligence`; checked 2026-05-21.	defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication; OASIS CTI standard for expressing cyber threat and observable information with structured objects, relationships, sightings, and markings.
What does the module inherit from `official_oasis_taxii_21` for **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**?	TAXII Version 2.1; lane `cyber_threat_intelligence`; checked 2026-05-21.	defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication; OASIS CTI transport standard for defensive threat-intelligence exchange channels, collections, discovery, and API contracts.
What does the module inherit from `official_mitre_attack_enterprise` for **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**?	MITRE ATT&CK Enterprise Matrix; lane `cyber_threat_intelligence`; checked 2026-05-21.	defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication; Threat-informed enterprise matrix for defensive TTP mapping, coverage analysis, detection engineering, and analytic normalization.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 21; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

21.3.8 Advanced Persistent Threats (APTs) assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 21; [237, 2026].

21.3.9 Advanced Persistent Threats (APTs) assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 21; [237, 2026].

21.3.9.1 Advanced Persistent Threats (APTs) capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis** and [237, 2026]; [258, 2026].

21.3.9.2 Advanced Persistent Threats (APTs) instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis** and [237, 2026]; [258, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

21.3.9.3 Advanced Persistent Threats (APTs) assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
APT Definitions, Lifecycle, and Attribution	Completed **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
APT Risk Propagation Models: ATT&CK-Based Analysis	Completed **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Nation-State vs. Ideological Actor Attack Patterns	Completed **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

21.3.10 Advanced Persistent Threats (APTs) refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [237, 2026]; [258, 2026] and **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**.

21.3.10.1 Advanced Persistent Threats (APTs) refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**. The local signals begin with [237, 2026]; [258, 2026].

21.3.10.2 Advanced Persistent Threats (APTs) claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**, and the source spine for these checks begins with [237, 2026]; [258, 2026].

21.3.11 Advanced Persistent Threats (APTs) reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [237, 2026]; [258, 2026].

Triangulation anchors. In module 13's review-checklist section, directly verified anchors for the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane include [of Standards and Technology, 2016]; [Committee, 2025]; [Committee, 2021]; [MITRE, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis**. [237, 2026]; [258, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

21.3.12 Advanced Persistent Threats (APTs) learning-path links: module map, overview, and curriculum atlas

Follow the cross-links to move between **APT Definitions, Lifecycle, and Attribution; APT Risk Propagation Models: ATT&CK-Based Analysis** and the rest of the curriculum without losing the source spine: orientation first, then the parent unit, then the modules on either side. Primary sources: [237, 2026]; [258, 2026].

Section 2, Section 19, Section 20, Section 22

22 Supply Chain Intelligence Attacks

22.0.1 Supply Chain Intelligence Attacks figures and course links: visual evidence, source flow, and navigation

The module uses Figure 56 and Figure 52 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.

Navigation links: Section 2, Section 19, Section 21, Section 23.

This module teaches the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane through a bounded, source-backed coursebook chapter. [258, 2026]; [266, 2026].

22.1 Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense frame for Supply Chain Intelligence Attacks: source context, topic focus, and reader task

Evidence anchor. Section 22; [258, 2026].

22.1.1 Supply Chain Intelligence Attacks orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 22; [258, 2026].

22.1.2 Supply Chain Intelligence Attacks conceptual primer: source context, core model, and reader task

This chapter teaches cyber threat intelligence as defensive normalization: incidents, indicators, TTPs, vendor risks, and sharing rules become useful only when scoped and validated. The chapter uses **Software-Supply-Chain Assurance Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**.

The central distinction is to separate defensive mapping and incident learning from exploit, persistence, or evasion instruction. Core topics include **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation; XZ Utils maintainer-trust case review for software supply-chain governance**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.

Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [of Standards and Technology, 2016]; [Committee, 2025]; [Committee, 2021]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [258, 2026]; [266, 2026].

Learners move from vocabulary and the **Software-Supply-Chain Assurance Lens** distinction through topic lessons on **Supply Chain Operations as Strategic Intelligence Tradecraft** with evidence and misconception checks, then assemble a **software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps** with safety and rights gates.

22.1.3 Supply Chain Intelligence Attacks learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 22; [258, 2026].

- Connect **Supply Chain Operations as Strategic Intelligence Tradecraft and SolarWinds/SUNBURST: The Six-Month Patient Operation** to **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate defensive mapping and incident learning from exploit, persistence, or evasion instruction; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as indicator fixation, unvetted sharing, vendor-assurance drift, weak incident scoping, and treating CTI as a feed instead of a workflow, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: cyber material stays defensive and tabletop-based; it does not provide exploit, persistence, evasion, or live-response instructions.

22.1.4 Supply Chain Intelligence Attacks core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 22; [258, 2026].

Term	Working definition
Indicator	an observable signal that may support defensive detection or investigation
TTP	a tactic, technique, or procedure used for structured defensive mapping
Sighting	a bounded observation of a possible indicator in a given context
Handling rule	a sharing, marking, or retention limit for threat information
Lessons learned	the post-incident evidence that changes controls or playbooks
Supply Chain Operations as Strategic…	Key terms: Supply, Chain, Operations.
SolarWinds/SUNBURST: The Six-Month Patient…	Key terms: SolarWinds, SUNBURST, Six.

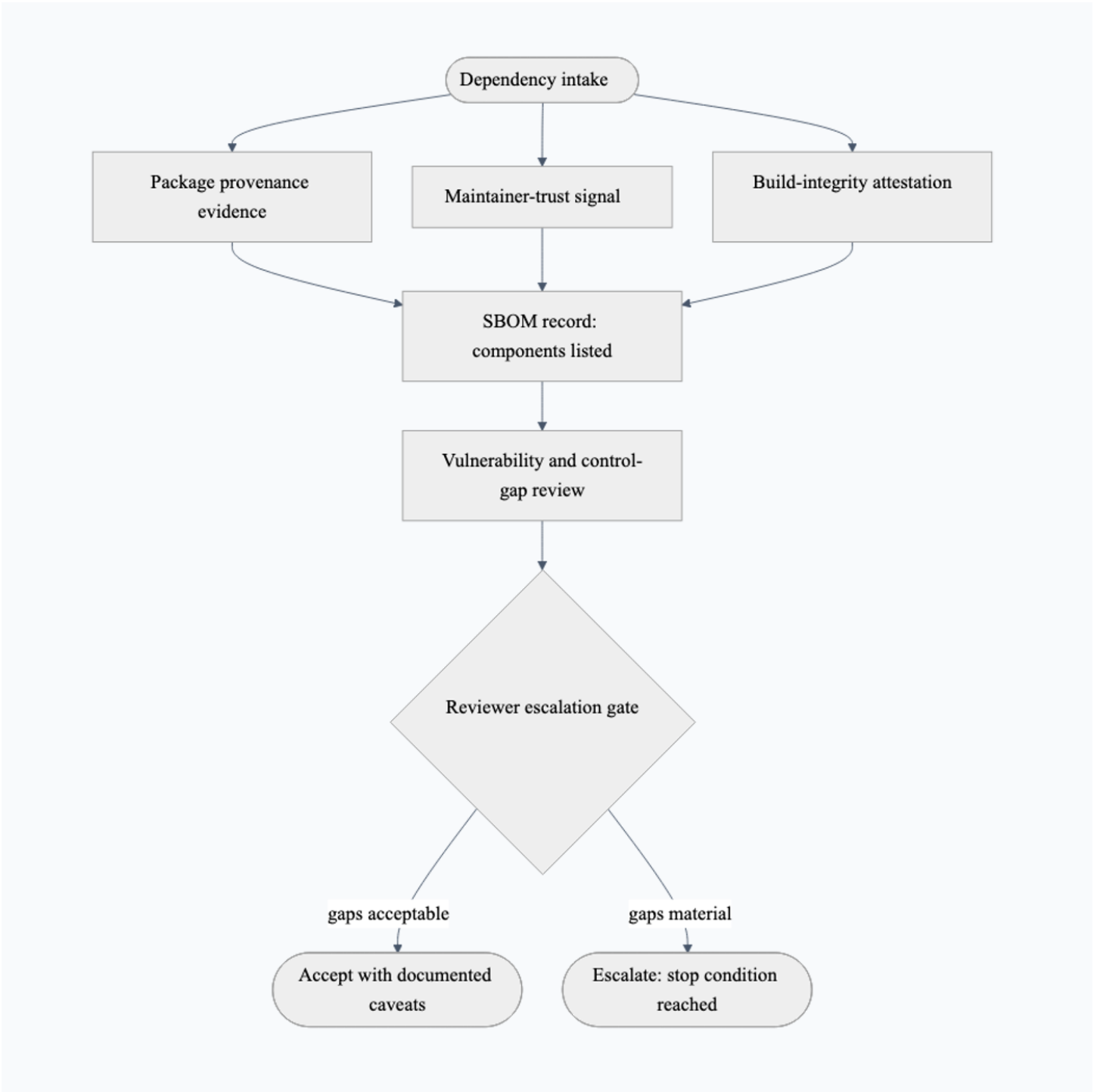


Figure 56: This diagram traces how package provenance, maintainer-trust signals, build integrity, and an SBOM converge into a reviewable assurance packet that names control gaps and an escalation boundary. It is anchored to the technical intelligence and cyber operations / supply chain intelligence attacks section; use it to inspect Dependency intake, Package provenance evidence, Maintainer-trust signal, and Build-integrity attestation while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

22.2 Software-Supply-Chain Assurance Lens path for Supply Chain Intelligence Attacks: lesson cluster, safe artifact, and review

Evidence anchor. Section 22; [258, 2026].

22.2.1 Supply Chain Intelligence Attacks practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 22; [258, 2026].

22.2.2 Supply Chain Intelligence Attacks topic lessons: source-backed concepts and transfer tasks

This module builds cyber threat intelligence as defensive normalization: incidents, indicators, TTPs, vendor risks, and sharing rules become useful only when scoped and validated. The sequence opens with **Supply Chain Operations as Strategic Intelligence Tradecraft**, **SolarWinds/SUNBURST: The Six-Month Patient Operation**, **XZ Utils maintainer-trust case review for software supply-chain governance** and applies the **Software-Supply-Chain Assurance Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 52; module overview Section 22; curriculum atlas Section 2.

Triangulation anchors. In module 14's topic-lessons section, directly verified anchors for the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane include [of Standards and Technology, 2016]; [Committee, 2025]; [Committee, 2021]; [MITRE, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

22.2.2.1 Lesson 1: Supply Chain Operations as Strategic Intelligence Tradecraft **Concept. Supply Chain Operations as Strategic Intelligence Tradecraft** shows how package provenance, social trust, build integrity, and assurance controls turn a software incident into reviewable evidence.

Why it matters. Without explicit treatment of **Supply Chain Operations**, indicator fixation undermines defensive CTI normalization and tabletop incident learning review; the lesson builds the habit to separate defensive mapping and incident learning from exploit, persistence, or evasion instruction.

Source support. Supply Chain Operations as Strategic Intelligence Tradecraft rests on [297, 2026] and [298, 2026]. The closest source to this row notes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for fixing what **Supply Chain Operations as Strategic Intelligence Tradecraft** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. Ground **Supply Chain Operations** in the evidence the row cites. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Supply Chain Operations**, build a **software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps** for this defensive CTI normalization and tabletop incident learning topic. The artifact must name the source descriptor, the bounded claim about **Supply Chain Operations as Strategic**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Supply Chain Operations** work as a **defensive CTI evidence packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that Supply Chain Operations as Strategic Intelligence Tradecraft replaces human review whenever evidence looks plausible.

Transfer task. Transfer **Supply Chain Operations** to a second module by preserving defensive CTI normalization and tabletop incident learning, changing the source evidence, and naming a new reviewer.

22.2.2.2 Lesson 2: SolarWinds/SUNBURST: The Six-Month Patient Operation **Concept. SolarWinds/SUNBURST: The Six-Month Patient Operation** shows how package provenance, social trust, build integrity, and assurance controls turn a software incident into reviewable evidence.

Why it matters. Analysts use **SolarWinds/SUNBURST** to separate defensive mapping and incident learning from exploit, persistence, or evasion instruction. A defensible treatment names the judgment it enables for defensive CTI normalization and tabletop incident learning review, the proof limit that indicator fixation would otherwise hide, and the reviewer accountable for challenge.

Source support. SolarWinds/SUNBURST: The Six-Month Patient Operation rests on [073, 2026]. Its anchor reference records: It explains how attackers compromised SolarWinds' Orion monitoring software with malicious code that spread to roughly 18,000 customers through software updates beginning in early 2020, and notes the attack's extended timeline and impact on U.S. Use it for fixing what **SolarWinds/SUNBURST: The Six-Month Patient Operation** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. Read **SolarWinds/SUNBURST** against the works cited for this row. [073, 2026] This Fortinet cybersecurity glossary page provides educational material about the SolarWinds supply chain attack. It explains how attackers compromised SolarWinds' Orion monitoring software with malicious code that spread to roughly 18,000 customers through software updates beginning in early 2020, and notes the attack's extended timeline and impact on U.S. federal agencies and major companies. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **SolarWinds/SUNBURST**, build a **software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps** for this defensive CTI normalization and tabletop incident learning topic. The artifact must name the source descriptor, the bounded claim about **SolarWinds/SUNBURST**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **SolarWinds/SUNBURST** work as a **defensive CTI evidence packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that SolarWinds/SUNBURST: The Six-Month Patient Operation can be used while ignoring the rule to separate defensive mapping and incident learning from exploit, persistence, or evasion instruction.

Transfer task. Transfer **SolarWinds/SUNBURST** to a second module by preserving defensive CTI normalization and tabletop incident learning, changing the source evidence, and naming a new reviewer.

22.2.2.3 Lesson 3: XZ Utils maintainer-trust case review for software supply-chain governance **Concept. XZ Utils maintainer-trust case review for software supply-chain governance** shows how package provenance, social trust, build integrity, and assurance controls turn a software incident into reviewable evidence.

Why it matters. XZ Utils maintainer-trust case review connects classroom vocabulary to Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. XZ Utils maintainer-trust case review for software supply-chain governance rests on [074, 2026], [075, 2026], and [076, 2026]. The closest source to this row notes: It describes how malicious code was hidden in test files and assembled only during compilation, potentially enabling unauthenticated remote code execution via OpenSSH, and how a long-term contributor gradually gained maintainer trust before inserting it. Use them for fixing what **XZ Utils maintainer-trust case review for software supply-chain governance** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. Ground **XZ Utils maintainer-trust case review** in the evidence the row cites. [074, 2026] A Vectra AI blog post from April 2024 analyzing the XZ Utils backdoor, a malicious commit discovered on March 29, 2024 in a widely used open-source compression library that could compromise affected systems via SSH. The article frames the incident as a supply chain compromise affecting both open-source and commercial software, drawing comparison to SolarWinds. [075, 2026] An Invicti Security blog post from April 2024 analyzing the xz-utils backdoor, a software supply chain compromise discovered in versions 5.6.0 and 5.6.1 of the compression library. It describes how malicious code was hidden in test files and assembled only during compilation, potentially enabling unauthenticated remote code execution via OpenSSH, and how a long-term contributor gradually gained maintainer trust before inserting it. [076, 2026] In early 2024, a malicious backdoor was discovered embedded in XZ Utils, a widely used compression library in Linux distributions, designed to enable unauthorized remote code execution via OpenSSH using an Ed448 private key. The perpetrator, operating under the pseudonym Jia Tan, spent over two years building trust as a contributor before inserting the exploit, which received a maximum CVSS score of 10.0. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **XZ Utils maintainer-trust case review**, build a maintainer-trust evidence card with provenance, communication-risk signal, uncertainty, and escalation boundary. Shape **XZ Utils maintainer-trust case review** work as a **defensive CTI evidence packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that a familiar maintainer name or popular package is a substitute for verifying provenance, integrity, and the chain of trust.

Transfer task. Transfer **XZ Utils maintainer-trust case review** from this module to a second motif by preserving defensive CTI normalization and tabletop incident learning, replacing action with audit, and naming the blocked use.

22.2.2.4 Lesson 4: Maintainer-contact provenance review for software supply-chain governance

Concept. Maintainer-contact provenance review for software supply-chain governance treats human-source work as a governed relationship: validation, consent, reporting, source protection, and oversight—not contact activity.

Why it matters. Without explicit treatment of **Maintainer-contact provenance review**, indicator fixation undermines defensive CTI normalization and tabletop incident learning review; the lesson builds the habit to separate defensive mapping and incident learning from exploit, persistence, or evasion instruction.

Source support. Maintainer-contact provenance review for software supply-chain governance rests on [076, 2026]. The closest source to this row notes: In early 2024, a malicious backdoor was discovered embedded in XZ Utils, a widely used compression library in Linux distributions, designed to enable unauthorized remote code execution via OpenSSH using an Ed448 private key. Use it for the claim that **Maintainer-contact provenance review for software supply-chain governance** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. For **Maintainer-contact provenance review**, reason from the sources cited in this row. [076, 2026] In early 2024, a malicious backdoor was discovered embedded in XZ Utils, a widely used compression library in Linux distributions, designed to enable unauthorized remote code execution via OpenSSH using an Ed448 private key. The perpetrator, operating under the pseudonym Jia Tan, spent over two years building trust as a contributor before inserting the exploit, which received a maximum CVSS score of 10.0. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Maintainer-contact provenance review**, build a maintainer-trust evidence card with provenance, communication-risk signal, uncertainty, and escalation boundary. Shape **Maintainer-contact provenance review** work as a **defensive CTI evidence packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that a familiar maintainer name or popular package is a substitute for verifying provenance, integrity, and the chain of trust.

Transfer task. Apply this module's safe boundary for **Maintainer-contact provenance review** to another artifact while keeping defensive CTI normalization and tabletop incident learning and reviewer ownership explicit.

22.2.2.5 Lesson 5: CVE-2024-3094: CVSS 10.0 Backdoor Mechanism

Concept. CVE-2024-3094: CVSS 10.0 Backdoor Mechanism treats the vulnerability record as an assurance case: severity, affected component, provenance, mitigation status, and uncertainty stay separate.

Why it matters. CVE-2024-3094 matters in the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane because defensive CTI normalization and tabletop incident learning evidence must stay separate from judgment; indicator fixation is a common failure.

Source support. CVE-2024-3094: CVSS 10.0 Backdoor Mechanism rests on [076, 2026]. The most specific cited work observes: In early 2024, a malicious backdoor was discovered embedded in XZ Utils, a widely used compression library in Linux distributions, designed to enable unauthorized remote code execution via OpenSSH using an Ed448 private key. Use it for the working definition that **CVE-2024-3094: CVSS 10.0 Backdoor Mechanism** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. Ground **CVE-2024-3094** in the evidence the row cites. [076, 2026] In early 2024, a malicious backdoor was discovered embedded in XZ Utils, a widely used compression library in Linux distributions, designed to enable unauthorized remote code execution via OpenSSH using an Ed448 private key. The perpetrator, operating under the pseudonym Jia Tan, spent over two years building trust as a contributor before inserting the exploit, which received a maximum CVSS score of 10.0. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **CVE-2024-3094**, build a **software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps** for this defensive CTI normalization and tabletop incident learning topic. The artifact must name the source descriptor, the bounded claim about **CVE**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **CVE-2024-3094** work as a **defensive CTI evidence packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that CVE-2024-3094: CVSS 10.0 Backdoor Mechanism replaces human review whenever evidence looks plausible.

Transfer task. Transfer **CVE-2024-3094** to a second module by preserving defensive CTI normalization and tabletop incident learning, changing the source evidence, and naming a new reviewer.

22.2.2.6 Lesson 6: Attribution Indicators: APT29/SVR Pattern Similarities

Concept. Attribution Indicators: APT29/SVR Pattern Similarities uses attribution indicators cautiously by separating technical similarity, context, confidence, and geopolitical inference.

Why it matters. Attribution Indicators connects classroom vocabulary to Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Attribution Indicators: APT29/SVR Pattern Similarities rests on [076, 2026]. The lead source's own note reads: In early 2024, a malicious backdoor was discovered embedded in XZ Utils, a widely used compression library in Linux distributions, designed to enable

unauthorized remote code execution via OpenSSH using an Ed448 private key. Use it for the claim that **Attribution Indicators: APT29/SVR Pattern Similarities** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. For **Attribution Indicators**, reason from the sources cited in this row. [076, 2026] In early 2024, a malicious backdoor was discovered embedded in XZ Utils, a widely used compression library in Linux distributions, designed to enable unauthorized remote code execution via OpenSSH using an Ed448 private key. The perpetrator, operating under the pseudonym Jia Tan, spent over two years building trust as a contributor before inserting the exploit, which received a maximum CVSS score of 10.0. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Attribution Indicators**, build a **software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps** for this defensive CTI normalization and tabletop incident learning topic. The artifact must name the source descriptor, the bounded claim about **Attribution Indicators**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Attribution Indicators** work as a **defensive CTI evidence packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that Attribution Indicators: APT29/SVR Pattern Similarities can be used while ignoring the rule to separate defensive mapping and incident learning from exploit, persistence, or evasion instruction.

Transfer task. Transfer **Attribution Indicators** to a second module by preserving defensive CTI normalization and tabletop incident learning, changing the source evidence, and naming a new reviewer.

22.2.2.7 Lesson 7: Maintainer-pressure communication signature review for software supply-chain governance

Concept. Maintainer-pressure communication signature review for software supply-chain governance teaches defensive recognition of manipulation attempts using sample messages, consent boundaries, and reporting duties.

Why it matters. Analysts use **Maintainer-pressure communication signature review** to separate defensive mapping and incident learning from exploit, persistence, or evasion instruction. A defensible treatment names the judgment it enables for defensive CTI normalization and tabletop incident learning review, the proof limit that indicator fixation would otherwise hide, and the reviewer accountable for challenge.

Source support. Maintainer-pressure communication signature review for software supply-chain governance rests on [076, 2026]. The most specific cited work observes: In early 2024, a malicious backdoor was discovered embedded in XZ Utils, a widely used compression library in Linux distributions, designed to enable unauthorized remote code execution via OpenSSH using an Ed448 private key. Use it for fixing what **Maintainer-pressure communication signature review for software supply-chain governance** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. Read **Maintainer-pressure communication signature review** against the works cited for this row. [076, 2026] In early 2024, a malicious backdoor was discovered embedded in XZ Utils, a widely used compression library in Linux distributions, designed to enable unauthorized remote code execution via OpenSSH using an Ed448 private key. The perpetrator, operating under the pseudonym Jia Tan, spent over two years building trust as a contributor before inserting the exploit, which received a maximum CVSS score of 10.0. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Maintainer-pressure communication signature review**, build a maintainer-trust evidence card with provenance, communication-risk signal, uncertainty, and escalation boundary. Shape **Maintainer-pressure communication signature review** work as a **defensive CTI evidence packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that a familiar maintainer name or popular package is a substitute for verifying provenance, integrity, and the chain of trust.

Transfer task. Reuse the **Maintainer-pressure communication signature review** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

22.2.2.8 Lesson 8: Maintainer-risk escalation review for software supply-chain governance

Concept. Maintainer-risk escalation review for software supply-chain governance analyzes how trust, maintainer contact, and package provenance become supply-chain assurance evidence without contacting or profiling real maintainers.

Why it matters. Without explicit treatment of **Maintainer-risk escalation review**, indicator fixation undermines defensive CTI normalization and tabletop incident learning review; the lesson builds the habit to separate defensive mapping and incident learning from exploit, persistence, or evasion instruction.

Source support. Maintainer-risk escalation review for software supply-chain governance rests on [076, 2026]. The lead source's own note reads: In early 2024, a malicious backdoor was discovered embedded in XZ Utils, a widely used compression library in Linux distributions, designed to enable unauthorized remote code execution via OpenSSH using an Ed448 private key. Use it for the working definition that **Maintainer-risk escalation review for software supply-chain governance** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. Read **Maintainer-risk escalation review** against the works cited for this row. [076, 2026] In early 2024, a malicious backdoor was discovered embedded in XZ Utils, a widely used compression library in Linux distributions, designed to enable unauthorized remote code execution via OpenSSH using an Ed448 private key. The perpetrator, operating under the pseudonym Jia Tan, spent over two years building trust as a contributor before inserting the exploit, which received a maximum CVSS score of 10.0. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Maintainer-risk escalation review**, build a maintainer-trust evidence card with provenance, communication-risk signal, uncertainty, and escalation boundary. Shape **Maintainer-risk escalation review** work as a **defensive CTI evidence packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that a familiar maintainer name or popular package is a substitute for verifying provenance, integrity, and the chain of trust.

Transfer task. Reuse the **Maintainer-risk escalation review** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

22.2.2.9 Lesson 9: Countermeasures: SBOM, SLSA Framework, Sigstore

Concept. Countermeasures: SBOM, SLSA Framework, Sigstore shows how package provenance, social trust, build integrity, and assurance controls turn a software incident into reviewable evidence.

Why it matters. Without explicit treatment of **Countermeasures: SBOM, SLSA Framework, Sigstore**, indicator fixation undermines defensive CTI normalization and tabletop incident learning review; the lesson builds the habit to separate defensive mapping and incident learning from exploit, persistence, or evasion instruction.

Source support. Countermeasures: SBOM, SLSA Framework, Sigstore rests on [300, 2026], [304, 2026], and [306, 2026]. Its anchor reference records: NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Use them for the claim that **Countermeasures: SBOM, SLSA Framework, Sigstore** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. Ground **Countermeasures: SBOM, SLSA Framework, Sigstore** in the evidence the row cites. [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Countermeasures**, build a **software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps** for this defensive CTI normalization and tabletop incident learning topic. The artifact must name the source descriptor, the bounded claim about **Countermeasures**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Countermeasures: SBOM, SLSA Framework, Sigstore** work as a **defensive CTI evidence packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that Countermeasures: SBOM, SLSA Framework, Sigstore replaces human review whenever evidence looks plausible.

Transfer task. Transfer **Countermeasures: SBOM, SLSA Framework, Sigstore** to a second module by preserving defensive CTI normalization and tabletop incident learning, changing the source evidence, and naming a new reviewer.

22.2.2.10 Lesson 10: Threat Intelligence Sharing for ICS Supply Chain (arXiv Survey)

Concept. Threat Intelligence Sharing for ICS Supply Chain (arXiv Survey) shows how package provenance, social trust, build integrity, and assurance controls turn a software incident into reviewable evidence.

Why it matters. Threat Intelligence Sharing matters in the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane because defensive CTI normalization and tabletop incident learning evidence must stay separate from judgment; indicator fixation is a common failure.

Source support. Threat Intelligence Sharing for ICS Supply Chain (arXiv Survey) rests on [077, 2026]. The closest source to this row notes: An arXiv research paper presenting an evidence-driven analysis of why threat information sharing for industrial control systems remains ineffective. Use it for pinning down the scope of **Threat Intelligence Sharing for ICS Supply Chain (arXiv Survey)**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of Standards and Technology, 2016]; [Committee, 2025].

Evidence to inspect. For **Threat Intelligence Sharing**, reason from the sources cited in this row. [077, 2026] An arXiv research paper presenting an evidence-driven analysis of why threat information sharing for industrial control systems remains ineffective. Drawing on three major ICS attacks and a review of 196 procedure examples across 22 malware families, it identifies limitations including incomplete support in the STIX sharing standard, reliance on proprietary undocumented protocols, and insufficient technical detail in threat and vulnerability reports. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Threat Intelligence Sharing**, build a **software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps** for this defensive CTI normalization and tabletop incident learning topic. The artifact must name the source descriptor, the bounded claim about **Threat Intelligence Sharing for ICS**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Threat Intelligence Sharing** work as a **defensive CTI evidence packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that Threat Intelligence Sharing for ICS Supply Chain (arXiv Survey) can be used while ignoring the rule to separate defensive mapping and incident learning from exploit, persistence, or evasion instruction.

Transfer task. Transfer **Threat Intelligence Sharing** to a second module by preserving defensive CTI normalization and tabletop incident learning, changing the source evidence, and naming a new reviewer.

22.2.3 Supply Chain Intelligence Attacks worked safe example: synthetic inputs, evidence, and review

Worked example: a sample campus SOC reviews fabricated alert records after a tabletop incident. [258, 2026]; [266, 2026].

Triangulation anchors. In module 14's worked-example section, directly verified anchors for the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane include [of Standards and Technology, 2016]; [Committee, 2025]; [Committee, 2021]; [MITRE, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **defensive cyber intelligence normalization**. Learners use a **defensive CTI evidence packet** and keep this boundary visible: No exploit, persistence, evasion, scanning, or production response instructions.

Frame. The classroom question centers on **Supply Chain Operations as Strategic Intelligence Tradecraft**. Excluded actions stay explicit, and the **Software-Supply-Chain Assurance Lens** planning question is: Which package, maintainer signal, build artifact, provenance claim, and assurance control needs review?

Inputs. For the **Supply Chain Operations as Strategic Intelligence Tradecraft** scenario, use toy alerts, synthetic asset names, public ATT&CK technique descriptions, and a sharing-policy card. The Software-Supply-Chain Assurance Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Supply Chain Operations as Strategic Intelligence Tradecraft**, students normalize indicators, map TTPs defensively, rate confidence, mark sharing limits, and record lessons learned. Pause whenever an inference about Supply Chain Operations as Strategic Intelligence Tradecraft appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Supply Chain Operations as Strategic Intelligence Tradecraft** classroom scenario; unit artifact = defensive CTI evidence packet; evidence = allowed inputs; method = defensive CTI normalization and tabletop incident learning; output = a CTI packet with indicators, TTP mapping, confidence, handling rule, and remediation owner; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Supply Chain Operations as Strategic Intelligence Tradecraft** as "Software-Supply-Chain Assurance Lens confirms it" is not enough. The revision ties the claim to defensive CTI normalization and tabletop incident learning, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Supply Chain Operations as Strategic Intelligence Tradecraft** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

22.2.4 Supply Chain Intelligence Attacks practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Software-Supply-Chain Assurance Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**.

Triangulation anchors. In module 14's practice-sequence section, directly verified anchors for the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane include [of Standards and Technology, 2016]; [Committee, 2025]; [Committee, 2021]; [MITRE, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Supply Chain Operations as Strategic Intelligence Tradecraft, SolarWinds/SUNBURST: The Six-Month Patient Operation, XZ Utils maintainer-trust case review for software supply-chain governance; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane.
2. Frame	Answer the lens question: Which package, maintainer signal, build artifact, provenance claim, and assurance control needs review?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Supply Chain Operations as Strategic Intelligence Tradecraft: software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the defensive CTI evidence packet fields for Supply Chain Operations as Strategic Intelligence Tradecraft.	Unit profile note.	Evidence artifacts include indicator context, TTP mapping.
4. Challenge	Test the misconception that Supply Chain Operations as Strategic Intelligence Tradecraft replaces human review whenever evidence looks plausible.	Failure-mode note.	The artifact applies the key distinction: separate defensive mapping and incident learning from exploit, persistence, or evasion instruction.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

22.2.4.1 Supply Chain Intelligence Attacks instructor notes: source reasoning, review points, and studio focus Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**. [258, 2026]; [266, 2026].

22.2.4.2 Supply Chain Intelligence Attacks extension exercise: peer validation and refresh trigger review Evidence anchor. Section 22; [258, 2026].

Have learners swap artifacts and apply the **Software-Supply-Chain Assurance Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**.

22.2.5 Supply Chain Intelligence Attacks knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 22; [258, 2026].

1. Explain how **Supply Chain Operations as Strategic Intelligence Tradecraft** is defined here; name the source descriptor that supports the definition.
2. Contrast **Supply Chain Operations as Strategic Intelligence Tradecraft** with **SolarWinds/SUNBURST: The Six-Month Patient Operation** using the **Software-Supply-Chain Assurance Lens** artifact fields.
3. Identify one failure mode from the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which indicator is useful only after context and confidence are added?
5. Correct this misconception: that Supply Chain Operations as Strategic Intelligence Tradecraft replaces human review whenever evidence looks plausible.

22.2.5.1 Supply Chain Intelligence Attacks answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Supply Chain Operations as Strategic Intelligence Tradecraft** without source evidence, uncertainty, or a safe transfer task.

22.3 Supply Chain Intelligence Attacks assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 22; [258, 2026].

22.3.1 Supply Chain Intelligence Attacks evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 22; [258, 2026].

22.3.2 Supply Chain Intelligence Attacks transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 22; [258, 2026].

22.3.2.1 Supply Chain Intelligence Attacks lineage and source tradition: profile, concepts, and first anchors This sits in the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lineage: turning indicators, TTPs, incidents, vendor risk, and response lessons into shareable defensive intelligence with clear handling rules. [258, 2026]; [266, 2026].

22.3.2.2 Supply Chain Intelligence Attacks working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 22; [258, 2026].
The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**, with provenance and reviewability throughout.

22.3.2.3 Supply Chain Intelligence Attacks knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** fabricated alerts, public taxonomy labels, incident context, supplier evidence, and handling rules. [258, 2026]; [266, 2026].
- **Transforms:** indicator normalization, TTP mapping, confidence scoring, sharing review, and control-gap analysis.
- **Outputs:** defensive CTI packet, handling note, control implication, and incident-learning memo.
- **Failure modes:** exploit detail leakage, indicator fixation, unvetted sharing, and unsupported attribution.

22.3.2.4 Supply Chain Intelligence Attacks transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 22; [258, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**.
- **Evidence contract:** keep the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as defensive CTI packet, handling note, control implication, and incident-learning memo that another reviewer can audit.

22.3.2.5 Supply Chain Intelligence Attacks profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 22; [258, 2026].
The matched profile emphasizes turning indicators, TTPs, incidents, vendor risk, and response lessons into shareable defensive intelligence with clear handling rules. The method stack is threat-information sharing goals, indicator/TTP normalization, incident-response review, supply-chain risk assessment, and lessons learned; the local topic cluster is **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**.

22.3.3 Supply Chain Intelligence Attacks evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 22; [258, 2026].
Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** profile tells reviewers what evidence is strong enough for the module artifact built around **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**.

22.3.3.1 Supply Chain Intelligence Attacks guide source spine: inherited keys and local citation roles Primary guide citations: [258, 2026]; [266, 2026]; [268, 2026]; [274, 2026]; [278, 2026]; [280, 2026]; [287, 2026]; [288, 2026]; [295, 2026]; [073, 2026]; [074, 2026]; [075, 2026]; [076, 2026]; [077, 2026]; [297, 2026]; [298, 2026]; [300, 2026]; [304, 2026]; [306, 2026].

22.3.3.2 Supply Chain Intelligence Attacks verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [258, 2026]; [266, 2026].

Tier	What counts	How it is used
Source guide	[258, 2026]; [266, 2026]; [268, 2026]; [274, 2026]; [278, 2026]; [280, 2026]; [287, 2026]; [288, 2026]; [295, 2026]; [073, 2026]; [074, 2026]; [075, 2026]; [076, 2026]; [077, 2026]; [297, 2026]; [298, 2026]; [300, 2026]; [304, 2026]; [306, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 14's source-canon section, directly verified anchors for the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane include [of Standards and Technology, 2016]; [Committee, 2025]; [Committee, 2021]; [MITRE, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Maintenance rule: Perplexity may suggest candidates for **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation** and [258, 2026]; [266, 2026], but only directly verified source URLs are encoded as citations.

22.3.3.3 Supply Chain Intelligence Attacks intelligence practice lens: evidence artifact and safety check Practice lens: **Software-Supply-Chain Assurance Lens** for **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**. [258, 2026]; [266, 2026].

Planning question: Which package, maintainer signal, build artifact, provenance claim, and assurance control needs review?

Evidence artifact: software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps.

Validation rule: separate provenance evidence, social-trust signals, build controls, vulnerability claims, and attribution uncertainty. Applied to **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**.

Handoff contract: handoff preserves package identity, source evidence, build evidence, review owner, uncertainty, and remediation priority as separate fields.

Safety check: exclude exploit reproduction, maintainer targeting, backdoor mechanics, credential hunting, and live repository interference.

22.3.3.4 Supply Chain Intelligence Attacks runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 22; [258, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	14.99	14.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Supply Chain Intelligence Attacks to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Bounded autonomy, procurement, incident-response, and assurance studio	14.101	14.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Supply Chain Intelligence Attacks	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Model-card, recoverability, retention, and learner-support evidence package	14.102	14.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Supply Chain Intelligence Attacks	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Supply Chain Operations as Strategic Intelligence Tradecraft	14.1	14.1 Supply Chain Operations as Strategic Intelligence Tradecraft	Software-Supply-Chain Assurance Lens	software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps	exclude exploit reproduction, maintainer targeting, backdoor mechanics, credential hunting, and live repository interference

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
SolarWinds/SUNBURST: The Six-Month Patient Operation	14.2	14.2 SolarWinds/SUNBURST: The Six-Month Patient Operation	Software-Supply-Chain Assurance Lens	software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps	exclude exploit reproduction, maintainer targeting, backdoor mechanics, credential hunting, and live repository interference
XZ Utils maintainer-trust case review for software supply-chain governance	14.3	14.3 source title transformed into safe curriculum treatment; original: XZ Utils/Jia Tan: Two-Year Social Engineering and Trust Infiltration	Software-Supply-Chain Assurance Lens	software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps	exclude exploit reproduction, maintainer targeting, backdoor mechanics, credential hunting, and live repository interference
Maintainer-contact provenance review for software supply-chain governance	14.3.1	14.3.1 source title transformed into safe curriculum treatment; original: Sock Puppetry as HUMINT Cover Tradecraft	Software-Supply-Chain Assurance Lens	software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps	exclude exploit reproduction, maintainer targeting, backdoor mechanics, credential hunting, and live repository interference
CVE-2024-3094: CVSS 10.0 Backdoor Mechanism	14.3.2	14.3.2 CVE-2024-3094: CVSS 10.0 Backdoor Mechanism	Software-Supply-Chain Assurance Lens	software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps	exclude exploit reproduction, maintainer targeting, backdoor mechanics, credential hunting, and live repository interference
Attribution Indicators: APT29/SVR Pattern Similarities	14.3.3	14.3.3 Attribution Indicators: APT29/SVR Pattern Similarities	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Maintainer-pressure communication signature review for software supply-chain governance	14.3.4	14.3.4 source title transformed into safe curriculum treatment; original: “Friendly Yet Aggressive and Persistent” Social Engineering Signature	Software-Supply-Chain Assurance Lens	software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps	exclude exploit reproduction, maintainer targeting, backdoor mechanics, credential hunting, and live repository interference
Maintainer-risk escalation review for software supply-chain governance	14.4	14.4 source title transformed into safe curriculum treatment; original: Open-Source Maintainer Targeting as an Acquisition Operation	Software-Supply-Chain Assurance Lens	software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps	exclude exploit reproduction, maintainer targeting, backdoor mechanics, credential hunting, and live repository interference
Countermeasures: SBOM, SLSA Framework, Sigstore	14.5	14.5 Countermeasures: SBOM, SLSA Framework, Sigstore	Software-Supply-Chain Assurance Lens	software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps	exclude exploit reproduction, maintainer targeting, backdoor mechanics, credential hunting, and live repository interference
Threat Intelligence Sharing for ICS Supply Chain (arXiv Survey)	14.6	14.6 Threat Intelligence Sharing for ICS Supply Chain (arXiv Survey)	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions

22.3.3.5 Supply Chain Intelligence Attacks reusable subsection contract: topic rows, artifacts, and safety duties **Evidence anchor.** Section 22; [258, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Supply Chain Operations as Strategic Intelligence Tradecraft	Software-Supply-Chain Assurance Lens	software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps	exclude exploit reproduction, maintainer targeting, backdoor mechanics, credential hunting, and live repository interference
SolarWinds/SUNBURST: The Six-Month Patient Operation	Software-Supply-Chain Assurance Lens	software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps	exclude exploit reproduction, maintainer targeting, backdoor mechanics, credential hunting, and live repository interference

Lesson topic	Practice lens	Evidence artifact	Safety check
XZ Utils maintainer-trust case review for software supply-chain governance	Software-Supply-Chain Assurance Lens	software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps	exclude exploit reproduction, maintainer targeting, backdoor mechanics, credential hunting, and live repository interference
Maintainer-contact provenance review for software supply-chain governance	Software-Supply-Chain Assurance Lens	software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps	exclude exploit reproduction, maintainer targeting, backdoor mechanics, credential hunting, and live repository interference
CVE-2024-3094: CVSS 10.0 Backdoor Mechanism	Software-Supply-Chain Assurance Lens	software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps	exclude exploit reproduction, maintainer targeting, backdoor mechanics, credential hunting, and live repository interference
Attribution Indicators: APT29/SVR Pattern Similarities	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Maintainer-pressure communication signature review for software supply-chain governance	Software-Supply-Chain Assurance Lens	software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps	exclude exploit reproduction, maintainer targeting, backdoor mechanics, credential hunting, and live repository interference
Maintainer-risk escalation review for software supply-chain governance	Software-Supply-Chain Assurance Lens	software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps	exclude exploit reproduction, maintainer targeting, backdoor mechanics, credential hunting, and live repository interference
Countermeasures: SBOM, SLSA Framework, Sigstore	Software-Supply-Chain Assurance Lens	software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps	exclude exploit reproduction, maintainer targeting, backdoor mechanics, credential hunting, and live repository interference
Threat Intelligence Sharing for ICS Supply Chain (arXiv Survey)	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions

22.3.3.6 Supply Chain Intelligence Attacks annotated source ledger: real titles and local contribution Each source cited by this **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** module is paired below with its real title and a one-line note on what it contributes to **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**.

Source	Cited work	What it contributes	Status
[258, 2026]	OpenAPI Specification	The official OpenAPI Initiative publications page, serving as a central index for the OpenAPI Specification and related standards including the Arazzo and Overlay specifications. It provides access to multiple specification versions (2.0, 3.0, 3.1, and 3.2) and their corresponding downloadable schemas identified by release date, along with a registry of extensions, formats, media types, and other resources.	verified source-guide
[266, 2026]	PROV Overview	A W3C Working Group Note from 2013 that provides an overview and roadmap for the PROV family of specifications for representing and exchanging provenance information on the web. It defines provenance as information about the entities, activities, and people involved in producing data, used to assess quality, reliability, and trustworthiness.	verified source-guide

Source	Cited work	What it contributes	Status
[268, 2026]	Data Catalog Vocabulary (DCAT) Version 3	DCAT Version 3 is a W3C RDF vocabulary designed to facilitate interoperability between data catalogs published on the web, enabling organizations to describe datasets and data services using standardized terminology for improved discoverability and federated search. The specification organizes catalog metadata around seven core classes including Catalog, Dataset, Distribution, Data Service, and Dataset Series, drawing on established vocabularies such as Dublin Core and FOAF.	verified source-guide
[274, 2026]	CAST Universal Design for Learning Guidelines version 3.0	The official CAST website for the Universal Design for Learning (UDL) Guidelines version 3.0, released in 2024. The framework offers research-based guidance for designing inclusive learning environments and is organized around three principles: Engagement (motivation and emotional support), Representation (accessible presentation of information), and Action and Expression (diverse means of participation and communication).	verified source-guide
[278, 2026]	Recommendation of the Council on Public Procurement	The OECD Recommendation of the Council on Public Procurement (OECD/LEGAL/0411), a legal instrument adopted by the OECD Council in 2015 on the proposal of the Public Governance Committee. It frames public procurement as a pillar of strategic governance and service delivery and sets out principles for governments to follow.	verified source-guide
[280, 2026]	NIST SP 800-61 Rev. 3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management	NIST SP 800-61 Rev. 3, published April 2025, integrates incident response guidance into broader cybersecurity risk management aligned with the NIST Cybersecurity Framework 2.0, superseding the 2012 Rev. 2. The publication addresses cyber threat information sharing, incident handling and management practices, and procedures for detecting, responding to, and recovering from security incidents.	verified source-guide
[287, 2026]	Datasheets for Datasets	A 2018 arXiv paper proposing 'datasheets for datasets,' a standardized documentation framework for machine learning datasets modeled on electronic component datasheets. The authors argue the field lacks consistent dataset documentation, which creates risk in high-stakes applications, and propose that datasets be accompanied by documentation covering motivation, composition, collection process, recommended uses, and test results.	verified source-guide

Source	Cited work	What it contributes	Status
[288, 2026]	Algorithmic Transparency Recording Standard Hub	A GOV.UK collection page serving as the hub for the UK Algorithmic Transparency Recording Standard (ATRS), maintained by the Government Digital Service. It provides a standardized template for documenting public-sector use of algorithmic tools, completion guidance, policy on scope and compliance, and a searchable repository of published transparency records.	verified source-guide
[295, 2026]	M-25-22: Driving Efficient Acquisition of Artificial Intelligence in Government	OMB Memorandum M-25-22 (April 3, 2025), Driving Efficient Acquisition of Artificial Intelligence in Government, issued under Executive Order 13960 and related directives. It provides guidance to federal agencies for acquiring effective and trustworthy AI in a timely, cost-effective manner, and rescinds and replaces earlier memorandum M-24-18.	verified source-guide
[073, 2026]	SolarWinds Supply Chain Attack - Fortinet	This Fortinet cybersecurity glossary page provides educational material about the SolarWinds supply chain attack. It explains how attackers compromised SolarWinds' Orion monitoring software with malicious code that spread to roughly 18,000 customers through software updates beginning in early 2020, and notes the attack's extended timeline and impact on U.S. federal agencies and major companies.	verified source-guide
[074, 2026]	How to Protect Against a Supply Chain Compromise - Vectra AI	A Vectra AI blog post from April 2024 analyzing the XZ Utils backdoor, a malicious commit discovered on March 29, 2024 in a widely used open-source compression library that could compromise affected systems via SSH. The article frames the incident as a supply chain compromise affecting both open-source and commercial software, drawing comparison to SolarWinds.	verified source-guide
[075, 2026]	The Xz-Utils Backdoor: The Supply Chain RCE That Got Caught	An Invicti Security blog post from April 2024 analyzing the xz-utils backdoor, a software supply chain compromise discovered in versions 5.6.0 and 5.6.1 of the compression library. It describes how malicious code was hidden in test files and assembled only during compilation, potentially enabling unauthenticated remote code execution via OpenSSH, and how a long-term contributor gradually gained maintainer trust before inserting it.	verified source-guide
[076, 2026]	XZ Utils backdoor	In early 2024, a malicious backdoor was discovered embedded in XZ Utils, a widely used compression library in Linux distributions, designed to enable unauthorized remote code execution via OpenSSH using an Ed448 private key. The perpetrator, operating under the pseudonym Jia Tan, spent over two years building trust as a contributor before inserting the exploit, which received a maximum CVSS score of 10.0.	verified source-guide context; do not use as primary analytic support

Source	Cited work	What it contributes	Status
[077, 2026]	An Evidence-Driven Analysis of Threat Information Sharing	An arXiv research paper presenting an evidence-driven analysis of why threat information sharing for industrial control systems remains ineffective. Drawing on three major ICS attacks and a review of 196 procedure examples across 22 malware families, it identifies limitations including incomplete support in the STIX sharing standard, reliance on proprietary undocumented protocols, and insufficient technical detail in threat and vulnerability reports.	verified source-guide
[297, 2026]	Intelligence Community Directive 203: Analytic Standards	Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products.	original source-guide
[298, 2026]	Intelligence Community Directives	Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations.	original source-guide
[300, 2026]	MITRE ATLAS	MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy.	original source-guide
[304, 2026]	Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities	NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences.	verified source-guide
[306, 2026]	Artificial Intelligence	Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support.	original source-guide

Where this sits. This module's overview is Section 22; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

22.3.4 Supply Chain Intelligence Attacks governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 22; [258, 2026].

22.3.5 Supply Chain Intelligence Attacks analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 14's governance-boundary section, directly verified anchors for the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane include [of Standards and Technology, 2016]; [Committee, 2025]; [Committee, 2021]; [MITRE, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Research lane: **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** for **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**. [258, 2026]; [266, 2026].
Curriculum topic spine: Supply Chain Operations as Strategic Intelligence Tradecraft, **SolarWinds/SUNBURST: The Six-Month Patient Operation**, **XZ Utils maintainer-trust case review for software supply-chain governance**. **Verified anchor cluster:** [of Standards and Technology, 2016]; [Committee, 2025]; [Committee, 2021]; [MITRE, 2026b]; [Cybersecurity and Agency, 2026d]; [of Standards and Technology, 2025c]; [for Economic Co-operation and Development, 2025a].
Conceptual depth: turning indicators, TTPs, incidents, vendor risk, and response lessons into shareable defensive intelligence with clear handling rules.
Method stack: threat-information sharing goals, indicator/TTP normalization, incident-response review, supply-chain risk assessment, and lessons learned.
Composability contract: indicators, TTP mappings, affected assets, supplier evidence, response actions, and sharing constraints remain independently reusable.
Known failure modes: indicator fixation, unvetted sharing, vendor-assurance drift, weak incident scoping, and treating CTI as a feed instead of a workflow.
Defensive boundary: cyber material stays defensive and tabletop-based; it does not provide exploit, persistence, evasion, or live-response instructions. Applied to **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**.

Anchor	Why it matters here
[of Standards and Technology, 2016]	Official guidance for establishing threat-information sharing goals, communities, distribution rules, and defensive use of indicators and TTPs. Checked as of 2026-05-21; role: curriculum_anchor.
[Committee, 2025]	OASIS CTI standard for expressing cyber threat and observable information with structured objects, relationships, sightings, and markings. Checked as of 2026-05-21; role: curriculum_anchor.
[Committee, 2021]	OASIS CTI transport standard for defensive threat-intelligence exchange channels, collections, discovery, and API contracts. Checked as of 2026-05-21; role: curriculum_anchor.
[MITRE, 2026b]	Threat-informed enterprise matrix for defensive TTP mapping, coverage analysis, detection engineering, and analytic normalization. Checked as of 2026-05-21; role: curriculum_anchor.
[Cybersecurity and Agency, 2026d]	Official catalog for prioritizing known exploited vulnerabilities as defensive triage inputs, not as exploitation instructions. Checked as of 2026-05-21; role: curriculum_anchor.
[of Standards and Technology, 2025c]	Official incident-response profile for preparation, detection, response, recovery, and continuous improvement under CSF 2.0. Checked as of 2026-05-21; role: curriculum_anchor.
[for Economic Co-operation and Development, 2025a]	OECD policy paper proposing a common AI incident reporting framework for jurisdictions and sectors, including criteria for impact and risk characterization. Checked as of 2026-05-24; role: curriculum_anchor.

22.3.5.1 Supply Chain Intelligence Attacks evidence standard and citation floor: source families and discovery limits Official guidance supplies governance, safety, and legal constraints for the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [258, 2026]; [266, 2026].

22.3.6 Supply Chain Intelligence Attacks agentic boundary: assist, approve, block, and record

Evidence anchor. Section 22; [258, 2026].
AGEINT translation is bounded by the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**.

22.3.6.1 Supply Chain Intelligence Attacks permitted defensive utility: curriculum uses and safe outputs **Evidence anchor.** Section 22; [258, 2026].
The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**.

22.3.6.2 Supply Chain Intelligence Attacks excluded operational boundary: blocked actions and stop rules Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [258, 2026]; [266, 2026] and **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

22.3.7 Supply Chain Intelligence Attacks governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 22; [258, 2026].

Governance is practiced as a gate on the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane. Learners use the **Software-Supply-Chain Assurance Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**.

22.3.7.1 Supply Chain Intelligence Attacks governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [258, 2026]; [266, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** failure modes and the **Software-Supply-Chain Assurance Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

22.3.7.2 Supply Chain Intelligence Attacks evidence package handoff: appendices, records, and reuse **Evidence anchor.** Section 22; [258, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Software-Supply-Chain Assurance Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**.

22.3.7.3 Supply Chain Intelligence Attacks current-source assurance: verified anchors and local artifact fit The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**. [258, 2026]; [266, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_nist_sp_800_150` for **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**?	Guide to Cyber Threat Information Sharing, NIST SP 800-150; lane `cyber_threat_intelligence`; checked 2026-05-21.	software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps; Official guidance for establishing threat-information sharing goals, communities, distribution rules, and defensive use of indicators and TTPs.
What does the module inherit from `official_oasis_stix_21` for **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**?	STIX Version 2.1; lane `cyber_threat_intelligence`; checked 2026-05-21.	software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps; OASIS CTI standard for expressing cyber threat and observable information with structured objects, relationships, sightings, and markings.
What does the module inherit from `official_oasis_taxii_21` for **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**?	TAXII Version 2.1; lane `cyber_threat_intelligence`; checked 2026-05-21.	software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps; OASIS CTI transport standard for defensive threat-intelligence exchange channels, collections, discovery, and API contracts.
What does the module inherit from `official_mitre_attack_enterprise` for **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**?	MITRE ATT&CK Enterprise Matrix; lane `cyber_threat_intelligence`; checked 2026-05-21.	software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps; Threat-informed enterprise matrix for defensive TTP mapping, coverage analysis, detection engineering, and analytic normalization.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 22; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

22.3.8 Supply Chain Intelligence Attacks assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 22; [258, 2026].

22.3.9 Supply Chain Intelligence Attacks assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 22; [258, 2026].

22.3.9.1 Supply Chain Intelligence Attacks capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation** and [258, 2026]; [266, 2026].

22.3.9.2 Supply Chain Intelligence Attacks instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation** and [258, 2026]; [266, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

22.3.9.3 Supply Chain Intelligence Attacks assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Supply Chain Operations as Strategic Intelligence Tradecraft	Completed **software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
SolarWinds/SUNBURST: The Six-Month Patient Operation	Completed **software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
XZ Utils maintainer-trust case review for software supply-chain governance	Completed **software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

22.3.10 Supply Chain Intelligence Attacks refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [258, 2026]; [266, 2026] and **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**.

22.3.10.1 Supply Chain Intelligence Attacks refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**. The local signals begin with [258, 2026]; [266, 2026].

22.3.10.2 Supply Chain Intelligence Attacks claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**, and the source spine for these checks begins with [258, 2026]; [266, 2026].

22.3.11 Supply Chain Intelligence Attacks reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [258, 2026]; [266, 2026].

Triangulation anchors. In module 14's review-checklist section, directly verified anchors for the **Cyber Threat Intelligence, Incident Response, and Supply-Chain Defense** lane include [of Standards and Technology, 2016]; [Committee, 2025]; [Committee, 2021]; [MITRE, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation**. [258, 2026]; [266, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.

- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

22.3.12 Supply Chain Intelligence Attacks learning-path links: module map, overview, and curriculum atlas

Follow the cross-links to move between **Supply Chain Operations as Strategic Intelligence Tradecraft; SolarWinds/SUNBURST: The Six-Month Patient Operation** and the rest of the curriculum without losing the source spine: orientation first, then the parent unit, then the modules on either side. Primary sources: [258, 2026]; [266, 2026].

Section 2, Section 19, Section 21, Section 23

23 Electronic and Emanations Intelligence

23.0.1 Electronic and Emanations Intelligence figures and course links: visual evidence, source flow, and navigation

The module uses Figure 57 and Figure 52 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 19, Section 22, Section 24.
This module teaches the **Collection Management and Multi-INT Requirements Discipline** lane through a bounded, source-backed coursebook chapter. [255, 2026]; [256, 2026].

23.1 Collection Management and Multi-INT Requirements Discipline frame for Electronic and Emanations Intelligence: source context, topic focus, and reader task

Evidence anchor. Section 23; [255, 2026].

23.1.1 Electronic and Emanations Intelligence orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 23; [255, 2026].

23.1.2 Electronic and Emanations Intelligence conceptual primer: source context, core model, and reader task

This chapter teaches collection management as requirements discipline: a source method is considered only after the priority, authority, minimization rule, source risk, and evaluation plan are explicit. The chapter uses **Dissemination-and-Marking Control Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**.
The central distinction is to separate collection discipline concepts from operational recruitment, interception, or tasking procedures. Core topics include **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise; Tempest and Van Eck Radiation: SIGINT legal-authority and communications-security governance exercise**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [255, 2026]; [256, 2026].
Learners move from vocabulary and the **Dissemination-and-Marking Control Lens** distinction through topic lessons on **SIGINT legal-authority and communications-security governance exercise** with evidence and misconception checks, then assemble a **dissemination map with audience, caveat, marking, records, and feedback fields** with safety and rights gates.

23.1.3 Electronic and Emanations Intelligence learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 23; [255, 2026].

- Connect **SIGINT legal-authority and communications-security governance exercise and EMINT: SIGINT legal-authority and communications-security governance exercise** to **Collection Management and Multi-INT Requirements Discipline** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **dissemination map with audience, caveat, marking, records, and feedback fields** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate collection discipline concepts from operational recruitment, interception, or tasking procedures; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as opportunistic collection, priority drift, over-collection, weak minimization, source exposure, and confusing availability with authority, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: collection material remains doctrinal and governance-oriented; it does not teach recruitment, interception, surveillance, or tasking procedures.

23.1.4 Electronic and Emanations Intelligence core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 23; [255, 2026].

Term	Working definition
Priority	the relative importance of an intelligence question
Source discipline	a broad evidence channel such as HUMINT, SIGINT, GEOINT, OSINT, or FININT
Minimization	the rule that limits acquisition, retention, or use of unnecessary information
Source protection	the duty to reduce risk to people, methods, and sensitive relationships
Evaluation	the feedback step that tests whether the evidence satisfied the requirement
Gray-zone indicator	an observable signal of ambiguous coercion below armed conflict thresholds
Proxy pattern	a relationship suggesting indirect sponsorship without confirmed operational control
SIGINT legal-authority and…	Key terms: SIGINT, legal, authority.
EMINT: SIGINT legal-authority and…	Key terms: EMINT, SIGINT, legal.

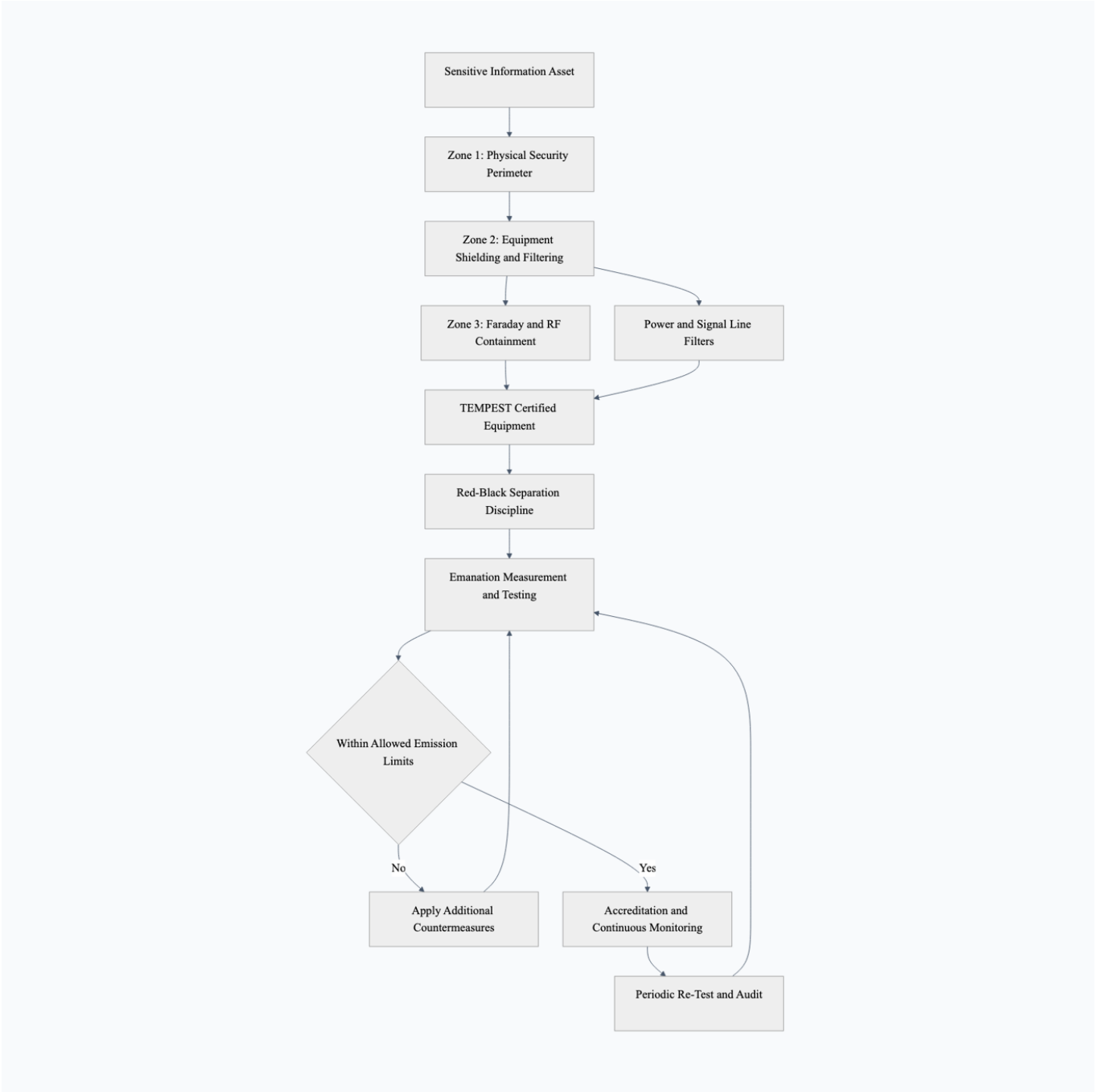


Figure 57: A defensive layered model showing how facilities contain compromising electromagnetic emanations through zoning, shielding, filtering, and continuous emission testing. The captioned view belongs to the technical intelligence and cyber operations / electronic and emanations intelligence section and should be read as a map of Sensitive Information Asset, Zone 1: Physical Security Perimeter, Zone 2: Equipment Shielding and Filtering, and Zone 3: Faraday and RF Containment, not as a capability score or live-task instruction.

23.2 Dissemination-and-Marking Control Lens path for Electronic and Emanations Intelligence: lesson cluster, safe artifact, and review

Evidence anchor. Section 23; [255, 2026].

23.2.1 Electronic and Emanations Intelligence practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 23; [255, 2026].

23.2.2 Electronic and Emanations Intelligence topic lessons: source-backed concepts and transfer tasks

This module builds collection management as requirements discipline: a source method is considered only after the priority, authority, minimization rule, source risk, and evaluation plan are explicit. The sequence opens with **SIGINT legal-authority and communications-security governance exercise**, **EMINT: SIGINT legal-authority and communications-security governance exercise**, **Tempest and Van Eck Radiation: SIGINT legal-authority and communications-security governance exercise** and applies the **Dissemination-and-Marking Control Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 52; module overview Section 23; curriculum atlas Section 2.

Triangulation anchors. In module 15's topic-lessons section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

23.2.2.1 Lesson 1: SIGINT legal-authority and communications-security governance exercise

Concept. SIGINT legal-authority and communications-security governance exercise distinguishes communications content from electronic signatures by evidence type, authority, minimization, and uncertainty.

Why it matters. SIGINT legal-authority connects classroom vocabulary to Collection Management and Multi-INT Requirements Discipline practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. SIGINT legal-authority and communications-security governance exercise rests on [035, 2026]. The closest source to this row notes: SIGINT is intelligence derived from electronic signals and systems used by foreign targets. Use it for pinning down the scope of **SIGINT legal-authority and communications-security governance exercise**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. Read **SIGINT legal-authority** against the works cited for this row. [035, 2026] SIGINT is intelligence derived from electronic signals and systems used by foreign targets. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **SIGINT legal-authority**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this requirements decomposition and source-discipline fit topic. The artifact must state the authority descriptor, the bounded claim about **SIGINT legal-authority and communications-security governance**, the minimization caveat, the uncertainty note, the collection boundary, and the reviewer accountable for the authorization. Shape **SIGINT legal-authority** work as a **defensive CTI evidence packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **SIGINT legal-authority**: that a named collection authority removes the minimization and retention limits on what may be kept.

Transfer task. Transfer **SIGINT legal-authority** from this module to a second motif by preserving requirements decomposition and source-discipline fit, replacing action with audit, and naming the blocked use.

23.2.2.2 Lesson 2: EMINT: SIGINT legal-authority and communications-security governance exercise

Concept. EMINT: SIGINT legal-authority and communications-security governance exercise frames SIGINT as authority-bound collection with minimization, handling rules, and communications-security implications.

Why it matters. EMINT: SIGINT legal-authority and communications-security governance exercise connects classroom vocabulary to Collection Management and Multi-INT Requirements Discipline practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. EMINT: SIGINT legal-authority and communications-security governance exercise rests on [078, 2026]. The lead source's own note reads: The book examines tradecraft, defined as the methods, practices, and techniques used in espionage and clandestine investigations. Use it for pinning down the scope of **EMINT: SIGINT legal-authority and communications-security governance exercise**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. Read **EMINT: SIGINT legal-authority and communications-security governance exercise** against the works cited for this row. [078, 2026] A Barnes & Noble listing for Advanced Criminal Investigations and Intelligence Operations by Robert J. Girod. The book examines tradecraft, defined as the methods, practices, and techniques used in espionage and clandestine investigations. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **EMINT**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this requirements decomposition and source-discipline fit topic. The artifact must state the authority descriptor, the bounded claim about **EMINT**, the minimization caveat, the uncertainty note, the collection boundary, and the reviewer accountable for the authorization. Shape **EMINT: SIGINT legal-authority and communications-security governance exercise** work as a **defensive CTI evidence packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **EMINT: SIGINT legal-authority and communications-security governance exercise**: that a named collection authority removes the minimization and retention limits on what may be kept.

Transfer task. Apply this module's safe boundary for **EMINT: SIGINT legal-authority and communications-security governance exercise** to another artifact while keeping requirements decomposition and source-discipline fit and reviewer ownership explicit.

23.2.2.3 Lesson 3: Tempest and Van Eck Radiation: SIGINT legal-authority and communications-security governance exercise

Concept. Tempest and Van Eck Radiation: SIGINT legal-authority and communications-security governance exercise frames SIGINT as authority-bound collection with minimization, handling rules, and communications-security implications.

Why it matters. Tempest and Van Eck Radiation matters in the **Collection Management and Multi-INT Requirements Discipline** lane because requirements decomposition and source-discipline fit evidence must stay separate from judgment; opportunistic collection is a common failure.

Source support. Tempest and Van Eck Radiation: SIGINT legal-authority and communications-security governance exercise rests on [300, 2026], [303, 2026], and [304, 2026]. The most specific cited work observes: It explains the benefits of SBOMs for vulnerability identification and supply-chain transparency, recommends machine-readable formats such as SPDX, CycloneDX, and SWID, and describes foundational, sustaining, and enhancing levels of implementation. Use them for the working definition that **Tempest and Van Eck Radiation: SIGINT legal-authority**

and communications-security governance exercise can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. For **Tempest and Van Eck Radiation**, reason from the sources cited in this row. [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. [303, 2026] An official NIST page on software supply chain security issued under Executive Order 14028, focused on the Software Bill of Materials as a formal record of software components and their supply chain. It explains the benefits of SBOMs for vulnerability identification and supply-chain transparency, recommends machine-readable formats such as SPDX, CycloneDX, and SWID, and describes foundational, sustaining, and enhancing levels of implementation. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Tempest and Van Eck Radiation**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this requirements decomposition and source-discipline fit topic. The artifact must state the authority descriptor, the bounded claim about **Tempest and Van Eck Radiation**, the minimization caveat, the uncertainty note, the collection boundary, and the reviewer accountable for the authorization. Shape **Tempest and Van Eck Radiation** work as a **defensive CTI evidence packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Tempest and Van Eck Radiation**: that a named collection authority removes the minimization and retention limits on what may be kept.

Transfer task. Transfer **Tempest and Van Eck Radiation** from this module to a second motif by preserving requirements decomposition and source-discipline fit, replacing action with audit, and naming the blocked use.

23.2.2.4 Lesson 4: RF-spectrum governance and communications-security

Concept. RF-spectrum governance and communications-security connects the technical term to authority, minimization, communications-security risk, and public doctrine rather than interception mechanics.

Why it matters. RF-spectrum governance connects classroom vocabulary to Collection Management and Multi-INT Requirements Discipline practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. RF-spectrum governance and communications-security rests on [303, 2026], [304, 2026], and [305, 2026]. Its anchor reference records: An official NIST page on software supply chain security issued under Executive Order 14028, focused on the Software Bill of Materials as a formal record of software components and their supply chain. Use them for the claim that **RF-spectrum governance and communications-security** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. For **RF-spectrum governance**, work from the cited evidence behind this row. [303, 2026] An official NIST page on software supply chain security issued under Executive Order 14028, focused on the Software Bill of Materials as a formal record of software components and their supply chain. It explains the benefits of SBOMs for vulnerability identification and supply-chain transparency, recommends machine-readable formats such as SPDX, CycloneDX, and SWID, and describes foundational, sustaining, and enhancing levels of implementation. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. [305, 2026] Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. Build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this requirements decomposition and source-discipline fit topic. The artifact must state the authority descriptor, the bounded claim about **RF-spectrum governance**, the minimization caveat, the uncertainty note, the collection boundary, and the reviewer accountable for the authorization. Shape this subject work as a **defensive CTI evidence packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **RF-spectrum governance**: that a named collection authority removes the minimization and retention limits on what may be kept.

Transfer task. Transfer **RF-spectrum governance** from this module to a second motif by preserving requirements decomposition and source-discipline fit, replacing action with audit, and naming the blocked use.

23.2.2.5 Lesson 5: RF Mapping and Spectrum Intelligence: RF-spectrum governance and communications-security

Concept. RF Mapping and Spectrum Intelligence: RF-spectrum governance and communications-security connects the technical term to authority, minimization, communications-security risk, and public doctrine rather than interception mechanics.

Why it matters. RF Mapping and Spectrum Intelligence connects classroom vocabulary to Collection Management and Multi-INT Requirements Discipline practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. RF Mapping and Spectrum Intelligence: RF-spectrum governance and communications-security rests on [302, 2026] and [297, 2026]. The most specific cited work observes: The official "About Us" page of the National Geospatial-Intelligence Agency (NGA), a U.S. Use them for pinning down the scope of **RF Mapping and Spectrum Intelligence: RF-spectrum governance and communications-security**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2026c].

Evidence to inspect. For **RF Mapping and Spectrum Intelligence**, work from the cited evidence behind this row. [302, 2026] The official "About Us" page of the National Geospatial-Intelligence Agency (NGA), a U.S. Department of Defense and intelligence community organization. It describes NGA's mission of delivering geospatial intelligence, or GEOINT, to support military operations, policymakers, and first responders, spanning imagery analysis, mapping, geodesy, and navigation safety. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **RF Mapping and Spectrum Intelligence**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this requirements decomposition and source-discipline fit topic. The artifact must state the authority descriptor, the bounded claim about **RF Mapping and Spectrum Intelligence**, the minimization caveat, the uncertainty note, the collection boundary, and the reviewer accountable for the authorization. Shape **RF Mapping and Spectrum Intelligence** work as a **defensive CTI evidence packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **RF Mapping and Spectrum Intelligence**: that a named collection authority removes the minimization and retention limits on what may be kept.

Transfer task. Transfer **RF Mapping and Spectrum Intelligence** from this module to a second motif by preserving requirements decomposition and source-discipline fit, replacing action with audit, and naming the blocked use.

23.2.3 Electronic and Emanations Intelligence worked safe example: synthetic inputs, evidence, and review

Worked example: a synthetic policy cell compares public indicators of hybrid pressure against an approved collection plan for a benign border-disruption exercise. [255, 2026]; [256, 2026].

Triangulation anchors. In module 15's worked-example section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **defensive cyber intelligence normalization**. Learners use a **defensive CTI evidence packet** and keep this boundary visible: No exploit, persistence, evasion, scanning, or production response instructions.

Frame. The classroom question centers on **SIGINT legal-authority and communications-security governance exercise**. Excluded actions stay explicit, and the **Dissemination-and-Marking Control Lens** planning question is: Which audience, release authority, marking vocabulary, records duty, and feedback loop governs this intelligence artifact?

Inputs. For the **SIGINT legal-authority and communications-security governance exercise** scenario, use public notices, synthetic interview summaries, public logistics records, and an instructor scope card. The Dissemination-and-Marking Control Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **SIGINT legal-authority and communications-security governance exercise**, students rank requirements, choose the least intrusive source discipline, list excluded actions, and evaluate evidence quality. Pause whenever an inference about SIGINT legal-authority and communications-security governance exercise appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **SIGINT legal-authority and communications-security governance exercise** classroom scenario; unit artifact = defensive CTI evidence packet; evidence = allowed inputs; method = requirements decomposition and source-discipline fit; output = a requirements-to-evidence matrix with discipline fit, source caveats, minimization notes, and gaps; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **SIGINT legal-authority and communications-security governance exercise** as "Dissemination-and-Marking Control Lens confirms it" is not enough. The revision ties the claim to requirements decomposition and source-discipline fit, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **SIGINT legal-authority and communications-security governance exercise** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

23.2.4 Electronic and Emanations Intelligence practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Dissemination-and-Marking Control Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**.

Triangulation anchors. In module 15's practice-sequence section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare SIGINT legal-authority and communications-security governance exercise, EMINT: SIGINT legal-authority and communications-security governance exercise, Tempest and Van Eck Radiation: SIGINT legal-authority and communications-security governance exercise; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Collection Management and Multi-INT Requirements Discipline** lane.
2. Frame	Answer the lens question: Which audience, release authority, marking vocabulary, records duty, and feedback loop governs this intelligence artifact?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for SIGINT legal-authority and communications-security governance exercise: dissemination map with audience, caveat, marking, records, and feedback fields.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the defensive CTI evidence packet fields for SIGINT legal-authority and communications-security governance exercise.	Unit profile note.	Evidence artifacts include indicator context, TTP mapping.
4. Challenge	Test the misconception that a named collection authority removes the minimization and retention limits on what may be kept.	Failure-mode note.	The artifact applies the key distinction: separate collection discipline concepts from operational recruitment, interception, or tasking procedures.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

23.2.4.1 Electronic and Emanations Intelligence instructor notes: source reasoning, review points, and studio focus

Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or

a human review point. Keep the focus on **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**. [255, 2026]; [256, 2026].

23.2.4.2 Electronic and Emanations Intelligence extension exercise: peer validation and refresh trigger review **Evidence anchor.** Section 23; [255, 2026].
Have learners swap artifacts and apply the **Dissemination-and-Marking Control Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**.

23.2.5 Electronic and Emanations Intelligence knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 23; [255, 2026].

1. Explain how **SIGINT legal-authority and communications-security governance exercise** is defined here; name the source descriptor that supports the definition.
2. Contrast **SIGINT legal-authority and communications-security governance exercise** with **EMINT: SIGINT legal-authority and communications-security governance exercise** using the **Dissemination-and-Marking Control Lens** artifact fields.
3. Identify one failure mode from the **Collection Management and Multi-INT Requirements Discipline** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which gray-zone indicator changes the least-intrusive source choice without crossing into operational tasking?
5. Correct this misconception: that a named collection authority removes the minimization and retention limits on what may be kept.

23.2.5.1 Electronic and Emanations Intelligence answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **SIGINT legal-authority and communications-security governance exercise** without source evidence, uncertainty, or a safe transfer task.

23.3 Electronic and Emanations Intelligence assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 23; [255, 2026].

23.3.1 Electronic and Emanations Intelligence evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 23; [255, 2026].

23.3.2 Electronic and Emanations Intelligence transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 23; [255, 2026].

23.3.2.1 Electronic and Emanations Intelligence lineage and source tradition: profile, concepts, and first anchors This sits in the **Collection Management and Multi-INT Requirements Discipline** lineage: requirements-driven, authority-bounded collection where priorities, legal basis, minimization, source protection, and evaluation are explicit. [255, 2026]; [256, 2026].

23.3.2.2 Electronic and Emanations Intelligence working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 23; [255, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**, with provenance and reviewability throughout.

23.3.2.3 Electronic and Emanations Intelligence knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** accountable requirements, source-discipline choices, minimization rules, source-risk notes, and evaluation criteria. [255, 2026]; [256, 2026].
- **Transforms:** priority mapping, source-discipline fit, least-intrusive evidence selection, and feedback review.
- **Outputs:** requirements matrix, collection-limit note, source-quality card, and gap list.
- **Failure modes:** recruitment or interception drift, over-collection, weak minimization, and source exposure.

23.3.2.4 Electronic and Emanations Intelligence transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 23; [255, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**.
- **Evidence contract:** keep the **Collection Management and Multi-INT Requirements Discipline** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as requirements matrix, collection-limit note, source-quality card, and gap list that another reviewer can audit.

23.3.2.5 Electronic and Emanations Intelligence profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 23; [255, 2026].

The matched profile emphasizes requirements-driven, authority-bounded collection where priorities, legal basis, minimization, source protection, and evaluation are explicit. The method stack is priority mapping, requirement decomposition, source-discipline fit, coverage-gap review, legal-authority check, and collection-feedback loop; the local topic cluster is **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**.

23.3.3 Electronic and Emanations Intelligence evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 23; [255, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Collection Management and Multi-INT Requirements Discipline** profile tells reviewers what evidence is strong enough for the module artifact built around **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**.

23.3.3.1 Electronic and Emanations Intelligence guide source spine: inherited keys and local citation roles Primary guide citations: [255, 2026]; [256, 2026]; [261, 2026]; [279, 2026]; [282, 2026]; [284, 2026]; [289, 2026]; [291, 2026]; [296, 2026]; [035, 2026]; [078, 2026]; [300, 2026]; [303, 2026]; [304, 2026]; [305, 2026]; [302, 2026]; [297, 2026].

23.3.3.2 Electronic and Emanations Intelligence verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [255, 2026]; [256, 2026].

Tier	What counts	How it is used
Source guide	[255, 2026]; [256, 2026]; [261, 2026]; [279, 2026]; [282, 2026]; [284, 2026]; [289, 2026]; [291, 2026]; [296, 2026]; [035, 2026]; [078, 2026]; [300, 2026]; [303, 2026]; [304, 2026]; [305, 2026]; [302, 2026]; [297, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 15's source-canon section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise** and [255, 2026]; [256, 2026], but only directly verified source URLs are encoded as citations.

23.3.3.3 Electronic and Emanations Intelligence intelligence practice lens: evidence artifact and safety check Practice lens: **Dissemination-and-Marking Control Lens** for **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**. [255, 2026]; [256, 2026].

Planning question: Which audience, release authority, marking vocabulary, records duty, and feedback loop governs this intelligence artifact?

Evidence artifact: dissemination map with audience, caveat, marking, records, and feedback fields.

Validation rule: verify source authority, public/classification status, CAPCO-safe vocabulary, audience need, and records disposition before reuse. Applied to **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**.

Handoff contract: deliver release-neutral summaries, source metadata, marking rationale, and review ownership as separate fields.

Safety check: exclude classified content, live release decisions, source-method exposure, and improvised control markings.

23.3.3.4 Electronic and Emanations Intelligence runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 23; [255, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	15.99	15.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Electronic and Emanations Intelligence to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Bounded autonomy, procurement, incident-response, and assurance studio	15.101	15.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Electronic and Emanations Intelligence	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Model-card, recoverability, retention, and learner-support evidence package	15.102	15.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Electronic and Emanations Intelligence	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
SIGINT legal-authority and communications-security governance exercise	15.1	15.1 source title transformed into safe curriculum treatment; original: ELINT: Radar Signatures and Weapons Systems Emissions	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
SIGINT legal-authority and communications-security governance exercise	15.2	15.2 source title transformed into safe curriculum treatment; original: EMINT: C4I System Emanations	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
SIGINT legal-authority and communications-security governance exercise	15.3	15.3 source title transformed into safe curriculum treatment; original: Tempest and Van Eck Radiation: Standards and Countermeasures	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
RF-spectrum governance and communications-security	15.4	15.4 source title transformed into safe curriculum treatment; original: Software-Defined Radio (SDR) for Intelligence Applications	AI/Data Accountability Lens	AI/data impact card with authority, provenance, model version, impact score, register status, human owner, and review cadence	reject automated adverse action, hidden surveillance expansion, unowned outputs, unreviewed model drift, and opaque downstream reuse
RF-spectrum governance and communications-security	15.5	15.5 source title transformed into safe curriculum treatment; original: RF Mapping and Spectrum Intelligence	AI/Data Accountability Lens	AI/data impact card with authority, provenance, model version, impact score, register status, human owner, and review cadence	reject automated adverse action, hidden surveillance expansion, unowned outputs, unreviewed model drift, and opaque downstream reuse

23.3.3.5 Electronic and Emanations Intelligence reusable subsection contract: topic rows, artifacts, and safety duties Evidence anchor. Section 23; [255, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
SIGINT legal-authority and communications-security governance exercise	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
EMINT: SIGINT legal-authority and communications-security governance exercise	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
Tempest and Van Eck Radiation: SIGINT legal-authority and communications-security governance exercise	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
RF-spectrum governance and communications-security	AI/Data Accountability Lens	AI/data impact card with authority, provenance, model version, impact score, register status, human owner, and review cadence	reject automated adverse action, hidden surveillance expansion, unowned outputs, unreviewed model drift, and opaque downstream reuse
RF Mapping and Spectrum Intelligence: RF-spectrum governance and communications-security	AI/Data Accountability Lens	AI/data impact card with authority, provenance, model version, impact score, register status, human owner, and review cadence	reject automated adverse action, hidden surveillance expansion, unowned outputs, unreviewed model drift, and opaque downstream reuse

23.3.3.6 Electronic and Emanations Intelligence annotated source ledger: real titles and local contribution Each source cited by this **Collection Management and Multi-INT Requirements Discipline** module is paired below with its real title and a one-line note on what it contributes to **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**.

Source	Cited work	What it contributes	Status
[255, 2026]	Web of Things (WoT) Architecture 1.1	The W3C Recommendation for Web of Things Architecture 1.1, published in December 2023, defining an abstract architecture for interoperability across diverse Internet of Things platforms. It introduces core concepts including Things described by machine-readable Thing Descriptions, reusable Thing Models, and Consumers that interpret descriptions to interact via Properties, Actions, and Events.	verified source-guide
[256, 2026]	Web of Things (WoT) Thing Description 1.1	The W3C WoT Thing Description 1.1 is a formal information model and standardized representation format enabling IoT devices to describe their metadata and interaction capabilities in a machine-readable way, facilitating interoperability across diverse ecosystems.	verified source-guide
[261, 2026]	RFC 9110: HTTP Semantics	RFC 9110, the official IETF standards document defining the core semantics and architecture of HTTP, published in June 2022 and consolidating nine earlier RFCs. It establishes terminology and protocol aspects shared across HTTP versions, including methods, status codes, header fields, content negotiation, conditional and range requests, authentication, and the http and https URI schemes.	verified source-guide
[279, 2026]	Open Contracting Data Standard	The documentation homepage for the Open Contracting Data Standard, version 1.1.5, maintained by the Open Contracting Partnership to support disclosure of government contracting data across the procurement lifecycle. It provides a common data model spanning planning, tender, award, contract, and implementation stages, along with a primer, implementation guidance, technical schemas, and validation tooling.	verified source-guide
[282, 2026]	AI Research: Security and Resilience	A NIST page on AI research focused on security and resilience, framing these as core characteristics of trustworthy AI under the NIST AI Risk Management Framework.	verified source-guide
[284, 2026]	Verifiable Credential Data Integrity 1.0	The W3C Recommendation for Verifiable Credential Data Integrity 1.0, published May 2025, defining mechanisms for ensuring the authenticity and integrity of verifiable credentials using cryptographic proofs. It specifies a process of data transformation, hashing, and proof generation, and a corresponding verification procedure, along with a proof data model containing properties such as type, verification method, purpose, and proof value.	verified source-guide

Source	Cited work	What it contributes	Status
[289, 2026]	Guidance for Organisations Using the Algorithmic Transparency Recording Standard	This is a GOV.UK guidance page published by the Government Digital Service that instructs public sector organizations on completing the Algorithmic Transparency Recording Standard (ATRS) template and publishing their records to the GOV.UK repository. It applies both to central government bodies required to publish under mandatory policy and to other public sector bodies doing so voluntarily.	verified source-guide
[291, 2026]	Revised 508 Standards and 255 Guidelines	Official documentation from the U.S. Access Board on the Revised 508 Standards and 255 Guidelines for information and communication technology accessibility. It establishes mandatory accessibility requirements for federal agencies and voluntary guidelines for telecommunications manufacturers, covering hardware, software, websites, electronic documents, and support services.	verified source-guide
[296, 2026]	Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile	NIST AI 600-1, the Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, a cross-sectoral companion resource to the NIST AI RMF 1.0 issued pursuant to Executive Order 14110. It identifies risks that are unique to or amplified by generative AI and organizes suggested actions for managing those risks, mapped to the AI RMF functions.	verified source-guide
[035, 2026]	Signals Intelligence (SIGINT) Overview	SIGINT is intelligence derived from electronic signals and systems used by foreign targets.	original source-guide
[078, 2026]	Advanced Criminal Investigations and Intelligence Operations: Tradecraft Methods, Practices, Tactics, and Techniques/Paperback	A Barnes & Noble listing for Advanced Criminal Investigations and Intelligence Operations by Robert J. Girod. The book examines tradecraft, defined as the methods, practices, and techniques used in espionage and clandestine investigations.	verified source-guide
[300, 2026]	MITRE ATLAS	MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy.	original source-guide
[303, 2026]	Software Security in Supply Chains	An official NIST page on software supply chain security issued under Executive Order 14028, focused on the Software Bill of Materials as a formal record of software components and their supply chain. It explains the benefits of SBOMs for vulnerability identification and supply-chain transparency, recommends machine-readable formats such as SPDX, CycloneDX, and SWID, and describes foundational, sustaining, and enhancing levels of implementation.	verified source-guide

Source	Cited work	What it contributes	Status
[304, 2026]	Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities	NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences.	verified source-guide
[305, 2026]	DevSecOps	Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support.	original source-guide
[302, 2026]	National Geospatial-Intelligence Agency About Us	The official "About Us" page of the National Geospatial-Intelligence Agency (NGA), a U.S. Department of Defense and intelligence community organization. It describes NGA's mission of delivering geospatial intelligence, or GEOINT, to support military operations, policymakers, and first responders, spanning imagery analysis, mapping, geodesy, and navigation safety.	verified source-guide
[297, 2026]	Intelligence Community Directive 203: Analytic Standards	Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products.	original source-guide

Where this sits. This module's overview is Section 23; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

23.3.4 Electronic and Emanations Intelligence governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 23; [255, 2026].

23.3.5 Electronic and Emanations Intelligence analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 15's governance-boundary section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **Collection Management and Multi-INT Requirements Discipline** for **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**. [255, 2026]; [256, 2026].

Curriculum topic spine: SIGINT legal-authority and communications-security governance exercise, **EMINT: SIGINT legal-authority and communications-security governance exercise**, **Tempest and Van Eck Radiation: SIGINT legal-authority and communications-security governance exercise**. **Verified anchor cluster:** [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]; [Archives and Administration, 1981]; [Agency, 2026g]; [of the Director of National Intelligence, 2026d].

Conceptual depth: requirements-driven, authority-bounded collection where priorities, legal basis, minimization, source protection, and evaluation are explicit.

Method stack: priority mapping, requirement decomposition, source-discipline fit, coverage-gap review, legal-authority check, and collection-feedback loop.

Composability contract: requirements, authorities, source disciplines, collection notes, retention limits, caveats, and evaluation metrics remain separable.

Known failure modes: opportunistic collection, priority drift, over-collection, weak minimization, source exposure, and confusing availability with authority.

Defensive boundary: collection material remains doctrinal and governance-oriented; it does not teach recruitment, interception, surveillance, or tasking procedures. Applied to **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**.

Anchor	Why it matters here
[Community, 2026]	Official public explanation of the intelligence cycle, collection disciplines, dissemination, evaluation, oversight, and partners. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026c]	Official prioritization directive for translating national intelligence priorities into collection, analysis, risk management, and responsiveness evaluation. Checked as of 2026-05-21; role: curriculum_anchor.
[of Staff, 2026]	Official joint-doctrine landing page for the keystone publication on joint intelligence principles, products, services, and assessments. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence and Agency, 2024]	Official IC OSINT strategy for professionalizing OSINT, integrated collection management, open-source sharing, innovation, and tradecraft. Checked as of 2026-05-21; role: curriculum_anchor.
[Archives and Administration, 1981]	Official legal anchor for intelligence authorities, rights-aware collection, analytic competition, oversight, and source-method protection. Checked as of 2026-05-21; role: curriculum_anchor.
[Agency, 2026g]	Official NSA public explanation of FISA oversight for signals intelligence collection governed by statutory and court-authorized controls. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026d]	Official sourcing directive for traceability, citations, source descriptors, and source summaries. Checked as of 2026-05-21; role: curriculum_anchor.

23.3.5.1 Electronic and Emanations Intelligence evidence standard and citation floor: source families and discovery limits Official guidance supplies governance, safety, and legal constraints for the **Collection Management and Multi-INT Requirements Discipline** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [255, 2026]; [256, 2026].

23.3.6 Electronic and Emanations Intelligence agentic boundary: assist, approve, block, and record

Evidence anchor. Section 23; [255, 2026].

AGEINT translation is bounded by the **Collection Management and Multi-INT Requirements Discipline** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**.

23.3.6.1 Electronic and Emanations Intelligence permitted defensive utility: curriculum uses and safe outputs **Evidence anchor.** Section 23; [255, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**.

23.3.6.2 Electronic and Emanations Intelligence excluded operational boundary: blocked actions and stop rules Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [255, 2026]; [256, 2026] and **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

23.3.7 Electronic and Emanations Intelligence governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 23; [255, 2026].
Governance is practiced as a gate on the **Collection Management and Multi-INT Requirements Discipline** lane. Learners use the **Dissemination-and-Marking Control Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**.

23.3.7.1 Electronic and Emanations Intelligence governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [255, 2026]; [256, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Collection Management and Multi-INT Requirements Discipline** failure modes and the **Dissemination-and-Marking Control Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

23.3.7.2 Electronic and Emanations Intelligence evidence package handoff: appendices, records, and reuse

Evidence anchor. Section 23; [255, 2026].
Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Dissemination-and-Marking Control Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**.

23.3.7.3 Electronic and Emanations Intelligence current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**. [255, 2026]; [256, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_intelligence_gov_how_ic_works` for **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**?	How the IC Works; lane `governed_intelligence_cycle`; checked 2026-05-21.	dissemination map with audience, caveat, marking, records, and feedback fields; Official public explanation of the intelligence cycle, collection disciplines, dissemination, evaluation, oversight, and partners.
What does the module inherit from `official_odni_icd_204` for **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**?	Intelligence Community Directive 204: National Intelligence Priorities Framework; lane `collection_management`; checked 2026-05-21.	dissemination map with audience, caveat, marking, records, and feedback fields; Official prioritization directive for translating national intelligence priorities into collection, analysis, risk management, and responsiveness evaluation.
What does the module inherit from `official_joint_pub_2_0` for **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**?	JP 2-0: Joint Intelligence; lane `collection_management`; checked 2026-05-21.	dissemination map with audience, caveat, marking, records, and feedback fields; Official joint-doctrine landing page for the keystone publication on joint intelligence principles, products, services, and assessments.
What does the module inherit from `official_ic_osint_strategy` for **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**?	The INT of First Resort: The IC OSINT Strategy 2024-2026; lane `osint_geoint`; checked 2026-05-21.	dissemination map with audience, caveat, marking, records, and feedback fields; Official IC OSINT strategy for professionalizing OSINT, integrated collection management, open-source sharing, innovation, and tradecraft.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 23; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

23.3.8 Electronic and Emanations Intelligence assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 23; [255, 2026].

23.3.9 Electronic and Emanations Intelligence assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 23; [255, 2026].

23.3.9.1 Electronic and Emanations Intelligence capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise** and [255, 2026]; [256, 2026].

23.3.9.2 Electronic and Emanations Intelligence instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise** and [255, 2026]; [256, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

23.3.9.3 Electronic and Emanations Intelligence assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
SIGINT legal-authority and communications-security governance exercise	Completed **dissemination map with audience, caveat, marking, records, and feedback fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
EMINT: SIGINT legal-authority and communications-security governance exercise	Completed **dissemination map with audience, caveat, marking, records, and feedback fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Tempest and Van Eck Radiation: SIGINT legal-authority and communications-security governance exercise	Completed **dissemination map with audience, caveat, marking, records, and feedback fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

23.3.10 Electronic and Emanations Intelligence refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [255, 2026]; [256, 2026] and **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**.

23.3.10.1 Electronic and Emanations Intelligence refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**. The local signals begin with [255, 2026]; [256, 2026].

23.3.10.2 Electronic and Emanations Intelligence claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**, and the source spine for these checks begins with [255, 2026]; [256, 2026].

23.3.11 Electronic and Emanations Intelligence reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [255, 2026]; [256, 2026].

Triangulation anchors. In module 15's review-checklist section, directly verified anchors for the **Collection Management and Multi-INT Requirements Discipline** lane include [Community, 2026]; [of the Director of National Intelligence, 2026c]; [of Staff, 2026]; [of the Director of National Intelligence and Agency, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise**. [255, 2026]; [256, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.

- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

23.3.12 Electronic and Emanations Intelligence learning-path links: module map, overview, and curriculum atlas

Follow the cross-links to move between **SIGINT legal-authority and communications-security governance exercise; EMINT: SIGINT legal-authority and communications-security governance exercise** and the rest of the curriculum without losing the source spine: orientation first, then the parent unit, then the modules on either side. Primary sources: [255, 2026]; [256, 2026].
Section 2, Section 19, Section 22, Section 24

24 IMAGERY AND FINANCIAL INTELLIGENCE

24.1 IMAGERY AND FINANCIAL INTELLIGENCE learning spine and source route: unit purpose, module order, and evidence handoff

Evidence anchor. Section 24; [253, 2026].

24.1.1 geospatial and financial intelligence uncertainty discipline spine: domain question and learning focus

Evidence anchor. Section 24; [253, 2026].
This unit teaches **geospatial and financial intelligence uncertainty**. GEOINT and FININT lessons teach spatial, temporal, and entity-risk reasoning while preserving uncertainty and compliance boundaries.

24.1.2 geospatial and financial intelligence uncertainty source-use contract: citation roles and evidence limits

Evidence anchor. Section 24; [253, 2026].
Use NGA definition and official compliance or due-diligence anchors for location quality, source limits, sanctions, ownership, and escalation claims.

24.1.3 geospatial and financial intelligence uncertainty practice artifact: recurring packet and retained evidence

Evidence anchor. Section 24; [253, 2026].
The recurring practice artifact is a **location-and-entity evidence ledger** that draws on geospatial quality note, temporal caveat, ownership uncertainty field, and escalation threshold. The unit keeps its learning spine explicit. Learners assess geospatial fitness, entity uncertainty, red flags, and the evidence needed before escalation.

24.1.4 geospatial and financial intelligence uncertainty safety boundary: accountable, synthetic, and evidence-bounded limits

No facility targeting, pattern-of-life inference, evasion advice, or attribution certainty beyond evidence.
This unit introduces the part's governing question, evidence artifacts, source-support spine, and capstone thread before the individual modules begin. [253, 2026]; [269, 2026].
Learners carry one unit capstone thread through the part: define an accountable intelligence question, bind it to source-quality constraints, produce a reviewable artifact, test the artifact against failure modes, and hand it off with enough context for another analyst or instructor to audit. The capstone remains public, synthetic, or owned-lab throughout; its first source anchors are [253, 2026]; [269, 2026].
This unit's deliverables are a source-canon card, claim/evidence ledger, safe-practice lab packet, failure-mode note, instructor rubric, and debrief memo. The full source-lane and evidence-package ledgers appear in the orientation and appendices; this unit introduction keeps only the learner-facing spine for [253, 2026]; [269, 2026].
This unit's safety gates are scope authorization, rights review, data provenance, tool allowlisting, human oversight, rollback, and evidence-bounded output. A missing gate turns the activity into a tabletop, audit, or written governance exercise until the gate is restored against [253, 2026]; [269, 2026].
Capstone thread:

Phase	Artifact	Review gate
Question	accountable learning question and excluded-action list	instructor confirms scope, allowed data, and rights impact
Source canon	source-lane map with guide citations, verified anchors, and refresh dates	citation keys resolve and source identity lock remains stable
Evidence ledger	claim, evidence, uncertainty, confidence, and reviewer register	every material claim has a source, caveat, and owner
Safe lab	synthetic or public dataset packet, tool allowlist, and stop conditions	no live target, private data, external action, or unsafe cyber-physical step
Assurance	evaluation rubric, failure-mode drill, rights map, and remediation note	human reviewer signs off before presentation or reuse
Debrief	capstone memo with lessons, residual risk, refresh triggers, and handoff owner	all unresolved questions and future approvals are explicit

Research lane: Open-Source and Geospatial Intelligence Integrity. Core anchors: [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]. Conceptual focus: public-source discovery converted into accountable intelligence through provenance, corroboration, minimization, and relevance tests. Composability contract: collection notes, source metadata, transformations, caveats, and analytic judgments remain separately exportable. **Practice lens:** Requirements-to-Evidence Lens; What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit? [253, 2026]; [269, 2026].

24.1.5 IMAGERY AND FINANCIAL INTELLIGENCE visual navigation and module map: evidence flow, order, and safety cues

The unit uses Figure 58 and Figure 59 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 23, Section 25.

24.1.6 IMAGERY AND FINANCIAL INTELLIGENCE module roster and source-lane inventory: citations, lanes, and learner route

Module	Section reference	Source spine
Imagery Intelligence (IMINT)	Section 25	[253, 2026]; [269, 2026]; [270, 2026]; [275, 2026]; [276, 2026]; [283, 2026]; [286, 2026]; [293, 2026]; [295, 2026]; [302, 2026]; [297, 2026]; [309, 2026]; [310, 2026]; [300, 2026].
Financial Intelligence (FININT)	Section 26	[251, 2026]; [252, 2026]; [254, 2026]; [273, 2026]; [274, 2026]; [275, 2026]; [286, 2026]; [287, 2026]; [292, 2026]; [079, 2026]; [080, 2026]; [081, 2026]; [082, 2026]; [302, 2026]; [297, 2026].

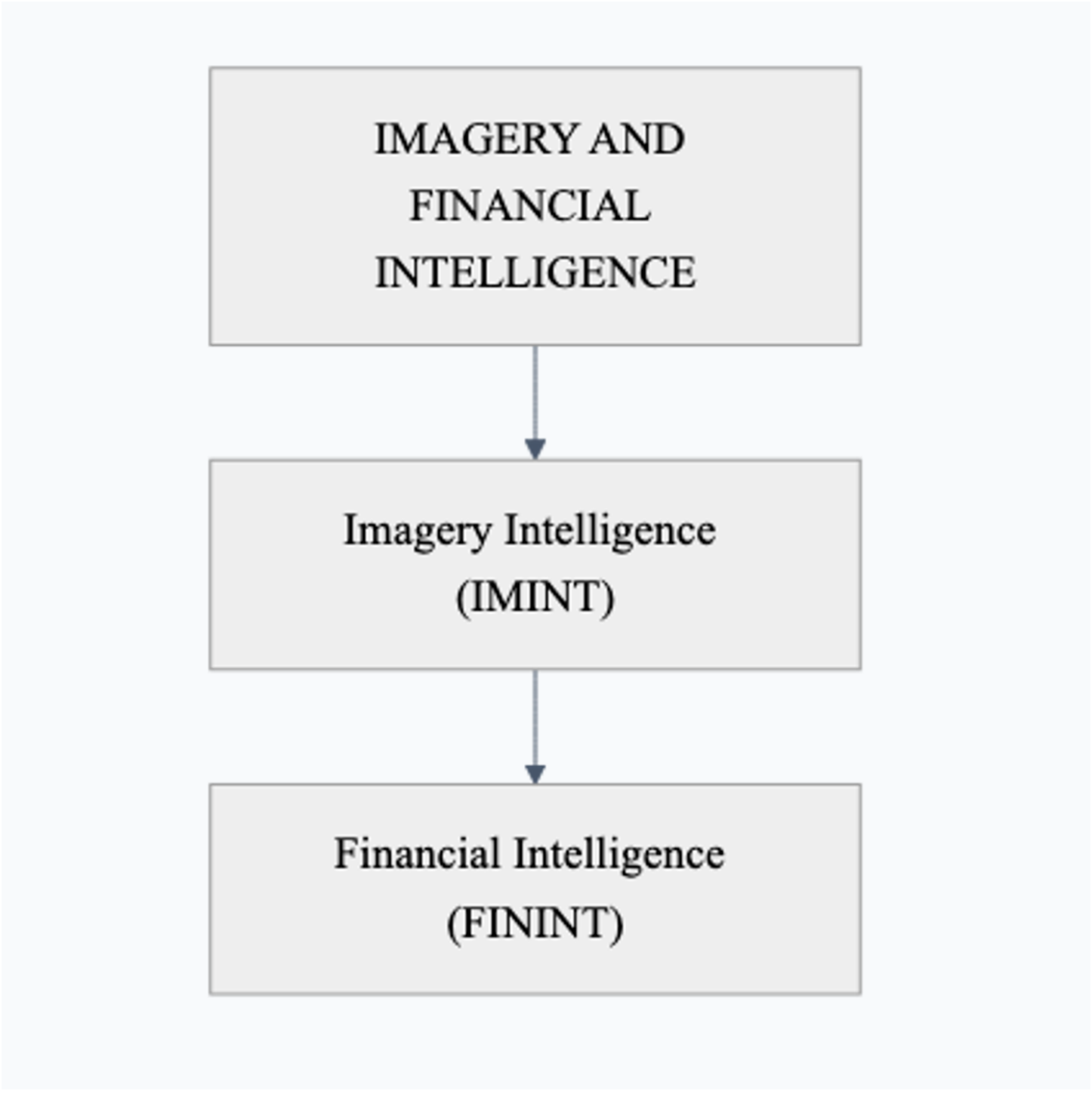


Figure 58: The unit module map traces the part's chapters as a linear reading sequence. Its reader value is to make 2 module nodes in the unit's ordered, source-backed reading sequence from its first module to its last visible at a glance, with the imagery and financial intelligence section as the source section and defensive review as the boundary.

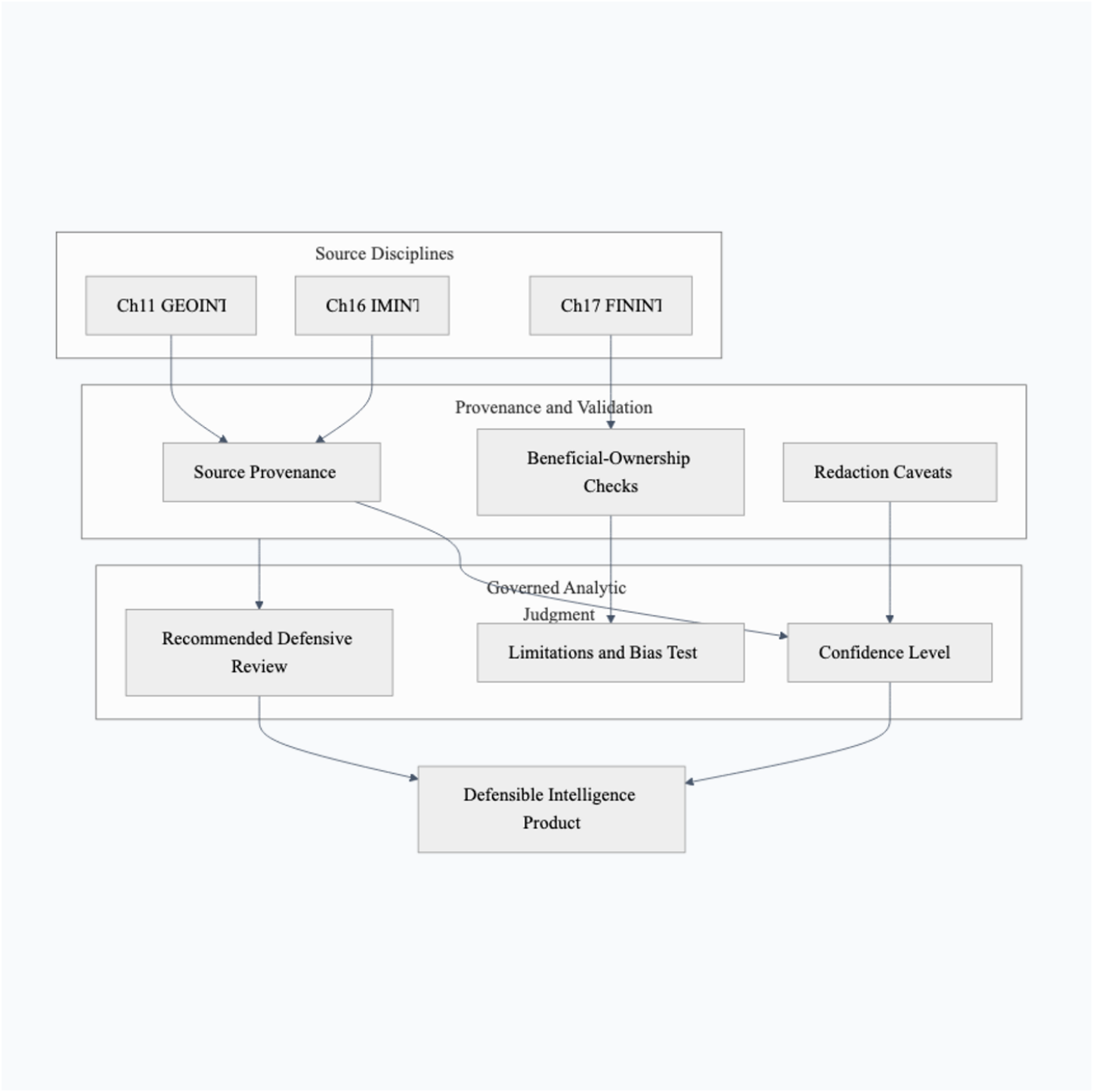


Figure 59: This Part traces how imagery and financial sources move left-to-right through provenance verification and validation gates before becoming a defensible analytic judgment. In the imagery and financial intelligence section, it lets readers compare Source Disciplines, Ch11 GEOINT, Ch16 IMINT, and Ch17 FININT so the visual functions as a traceable course aid rather than an unscoped assertion.

25 Imagery Intelligence (IMINT)

25.0.1 Imagery Intelligence (IMINT) figures and course links: visual evidence, source flow, and navigation

The module uses Figure 60, Figure 61, Figure 62, and Figure 58 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 24, Section 26.
This module teaches the **Open-Source and Geospatial Intelligence Integrity** lane through a bounded, source-backed coursebook chapter. [253, 2026]; [269, 2026].

25.1 Open-Source and Geospatial Intelligence Integrity frame for Imagery Intelligence (IMINT): source context, topic focus, and reader task

Evidence anchor. Section 25; [253, 2026].

25.1.1 Imagery Intelligence (IMINT) orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 25; [253, 2026].

25.1.2 Imagery Intelligence (IMINT) conceptual primer: source context, core model, and reader task

This chapter teaches OSINT and GEOINT as public-source reasoning disciplines: availability does not equal reliability, relevance, legality, or ethical reuse. The chapter uses **Requirements-to-Evidence Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**.
The central distinction is to separate discovery from collection expansion, and map or media interpretation from targeting. Core topics include **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs; Photo-interpretation literacy: resolution, uncertainty, and scale**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [253, 2026]; [269, 2026].
Learners move from vocabulary and the **Requirements-to-Evidence Lens** distinction through topic lessons on **Imagery modality literacy: resolution, scale, and sensor-fit** with evidence and misconception checks, then assemble a **requirements matrix with source descriptors, caveats, and collection limits** with safety and rights gates.

25.1.3 Imagery Intelligence (IMINT) learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 25; [253, 2026].

- Connect **Imagery modality literacy: resolution, scale, and sensor-fit and Imagery collection-platform literacy: resolution and revisit tradeoffs** to **Open-Source and Geospatial Intelligence Integrity** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **requirements matrix with source descriptors, caveats, and collection limits** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate discovery from collection expansion, and map or media interpretation from targeting; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as privacy drift, stale data, context collapse, platform bias, over-collection, and mistaking availability for reliability, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: OSINT work uses lawful public, owned-lab, or explicitly approved sources and avoids doxxing, harassment, live tracking, or operational targeting.

25.1.4 Imagery Intelligence (IMINT) core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 25; [253, 2026].

Term	Working definition
Provenance	the origin, chain, and transformation history of a source
Corroboration	the comparison of independent sources before reuse
Recency	the time relationship between source creation, discovery, and claim
Geospatial quality	accuracy, completeness, temporal fitness, and usability of location data
Minimization	limiting retained information to what the accountable question requires
Imagery modality literacy: resolution, scale,…	Key terms: Imagery, modality, literacy.
Imagery collection-platform literacy:…	Key terms: Imagery, collection, platform.

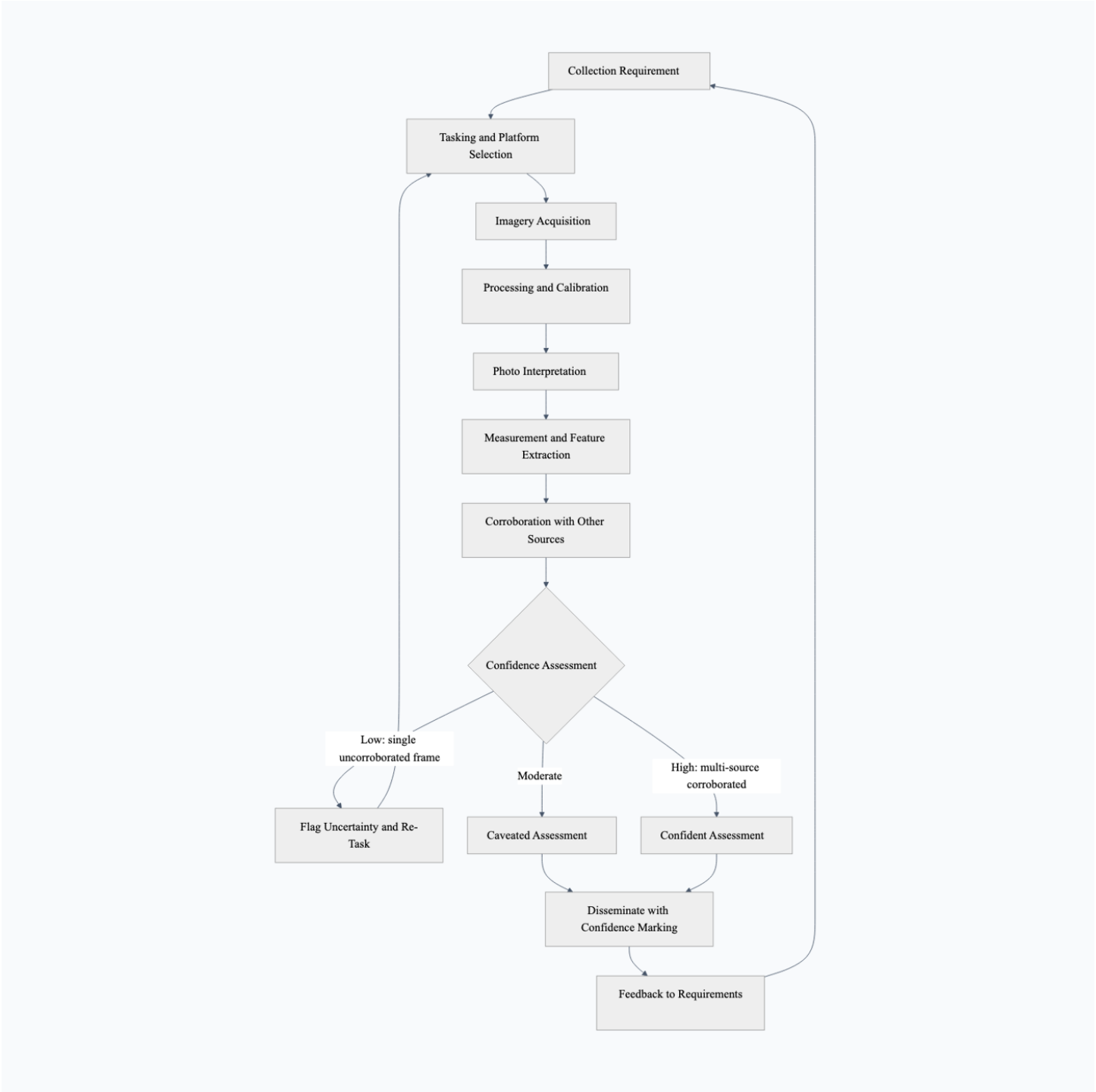


Figure 60: A requirements-to-evidence pipeline showing how imagery moves from tasking through interpretation to a graded confidence assessment before caveated dissemination. Its reader value is to make Collection Requirement, Tasking and Platform Selection, Imagery Acquisition, and Processing and Calibration visible at a glance, with the imagery and financial intelligence / imagery intelligence imint section as the source section and defensive review as the boundary.

Figure 61: Public-domain USGS EROS declassified HEXAGON image used as a historical example of imagery becoming a governed analytic source. Its reader value is to make U.S. Geological Survey provenance, 1973-03-20 collection context, public-domain status, and analytic reuse boundary visible at a glance, with the imagery and financial intelligence / imagery intelligence imint section as the source section and defensive review as the boundary.

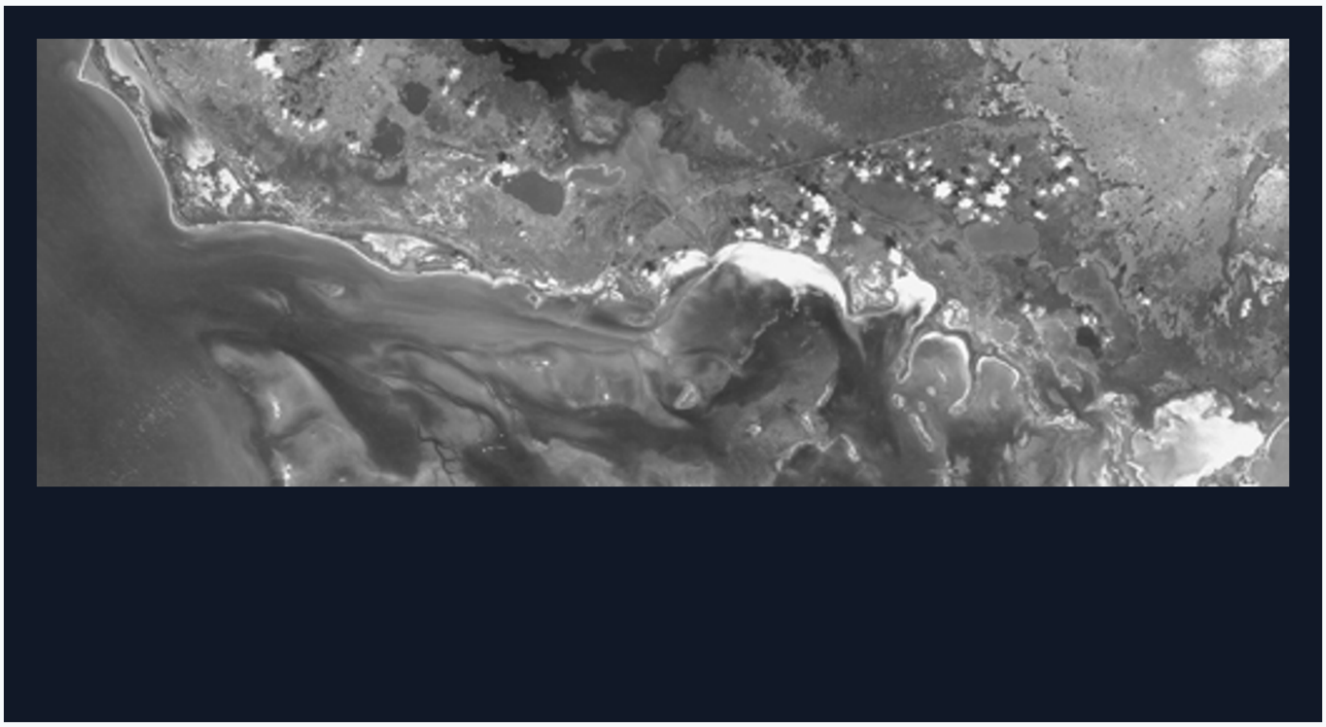


Figure 62: Public-domain USGS EROS KH-7 image used to show how historical collection becomes reproducible open-source imagery analysis. In the imagery and financial intelligence / imagery intelligence imint section, it lets readers compare U.S. Geological Survey provenance, 1966 approx. collection context, public-domain status, and analytic reuse boundary so the visual functions as a traceable course aid rather than an unscoped assertion.

25.2 Requirements-to-Evidence Lens path for Imagery Intelligence (IMINT): lesson cluster, safe artifact, and review

Evidence anchor. Section 25; [253, 2026].

25.2.1 Imagery Intelligence (IMINT) practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 25; [253, 2026].

25.2.2 Imagery Intelligence (IMINT) topic lessons: source-backed concepts and transfer tasks

This module builds OSINT and GEOINT as public-source reasoning disciplines: availability does not equal reliability, relevance, legality, or ethical reuse. The sequence opens with **Imagery modality literacy: resolution, scale, and sensor-fit**, **Imagery collection-platform literacy: resolution and revisit tradeoffs**, **Photo-interpretation literacy: resolution, uncertainty, and scale** and applies the **Requirements-to-Evidence Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 58; module overview Section 25; curriculum atlas Section 2.

Triangulation anchors. In module 16's topic-lessons section, directly verified anchors for the **Open-Source and Geospatial Intelligence Integrity** lane include [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]; [Agency, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

25.2.2.1 Lesson 1: Imagery modality literacy: resolution, scale, and sensor-fit

Concept. Imagery modality literacy: resolution, scale, and sensor-fit treats location evidence as a quality and uncertainty problem, separating map interpretation from targeting or attribution.

Why it matters. Analysts use **Imagery modality literacy** to separate discovery from collection expansion, and map or media interpretation from targeting. A defensible treatment names the judgment it enables for source-quality review and non-sensitive geospatial interpretation review, the proof limit that privacy drift would otherwise hide, and the reviewer accountable for challenge.

Source support. Imagery modality literacy: resolution, scale, and sensor-fit rests on [302, 2026] and [297, 2026]. The closest source to this row notes: Department of Defense and intelligence community organization. Use them for fixing what **Imagery modality literacy: resolution, scale, and sensor-fit** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. Read **Imagery modality literacy** against the works cited for this row. [302, 2026] The official "About Us" page of the National Geospatial-Intelligence Agency (NGA), a U.S. Department of Defense and intelligence community organization. It describes NGA's mission of delivering geospatial intelligence, or GEOINT, to support military operations, policymakers, and first responders, spanning imagery analysis, mapping, geodesy, and navigation safety. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Imagery modality literacy**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this source-quality review and non-sensitive geospatial interpretation topic. The artifact must list the imagery descriptor, the bounded claim about **Imagery modality literacy**, the resolution caveat, the uncertainty note, the sensitive-site boundary, and the reviewer who checks the interpretation. Shape **Imagery modality literacy** work as a **location-and-entity evidence ledger** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Imagery modality literacy**: that a visible feature is enough for a confident geospatial claim.

Transfer task. Apply this module's safe boundary for **Imagery modality literacy** to another artifact while keeping source-quality review and non-sensitive geospatial interpretation and reviewer ownership explicit.

25.2.2.2 Lesson 2: Imagery collection-platform literacy: resolution and revisit tradeoffs

Concept. Imagery collection-platform literacy: resolution and revisit tradeoffs treats location evidence as a quality and uncertainty problem, separating map interpretation from targeting or attribution.

Why it matters. Imagery collection-platform literacy matters in the **Open-Source and Geospatial Intelligence Integrity** lane because source-quality review and non-sensitive geospatial interpretation evidence must stay separate from judgment; privacy drift is a common failure.

Source support. Imagery collection-platform literacy: resolution and revisit tradeoffs rests on [309, 2026], [310, 2026], and [300, 2026]. The lead source's own note reads: The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. Use them for pinning down the scope of **Imagery collection-platform literacy: resolution and revisit tradeoffs**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. Ground **Imagery collection-platform literacy** in the evidence the row cites. [309, 2026] An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection. [310, 2026] The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Imagery collection-platform literacy**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this source-quality review and non-sensitive geospatial interpretation topic. The artifact must list the imagery descriptor, the bounded claim about **Imagery collection-platform literacy**, the resolution caveat, the uncertainty note, the sensitive-site boundary, and the reviewer who checks the interpretation. Shape **Imagery collection-platform literacy** work as a **location-and-entity evidence ledger** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Imagery collection-platform literacy**: that a visible feature is enough for a confident geospatial claim.

Transfer task. Transfer **Imagery collection-platform literacy** from this module to a second motif by preserving source-quality review and non-sensitive geospatial interpretation, replacing action with audit, and naming the blocked use.

25.2.2.3 Lesson 3: Photo-interpretation literacy: resolution, uncertainty, and scale

Concept. Photo-interpretation literacy: resolution, uncertainty, and scale treats location evidence as a quality and uncertainty problem, separating map interpretation from targeting or attribution.

Why it matters. Without explicit treatment of **Photo-interpretation literacy**, privacy drift undermines source-quality review and non-sensitive geospatial interpretation review; the lesson builds the habit to separate discovery from collection expansion, and map or media interpretation from targeting.

Source support. Photo-interpretation literacy: resolution, uncertainty, and scale rests on [302, 2026] and [297, 2026]. The closest source to this row notes: It describes NGA's mission of delivering geospatial intelligence, or GEOINT, to support military operations, policymakers, and first responders, spanning imagery analysis, mapping, geodesy, and navigation safety. Use them for the working definition that **Photo-interpretation literacy: resolution, uncertainty, and scale** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. For **Photo-interpretation literacy**, reason from the sources cited in this row. [302, 2026] The official "About Us" page of the National Geospatial-Intelligence Agency (NGA), a U.S. Department of Defense and intelligence community organization. It describes NGA's mission of delivering geospatial intelligence, or GEOINT, to support military operations, policymakers, and first responders, spanning imagery analysis, mapping, geodesy, and navigation safety. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Photo-interpretation literacy**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this source-quality review and non-sensitive geospatial interpretation topic. The artifact must list the imagery descriptor, the bounded claim about **Photo-interpretation literacy**, the resolution caveat, the uncertainty note, the sensitive-site boundary, and the reviewer who checks the interpretation. Shape **Photo-interpretation literacy** work as a **location-and-entity evidence ledger** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Photo-interpretation literacy**: that a visible feature is enough for a confident geospatial claim.

Transfer task. Apply this module's safe boundary for **Photo-interpretation literacy** to another artifact while keeping source-quality review and non-sensitive geospatial interpretation and reviewer ownership explicit.

25.2.2.4 Lesson 4: Commercial imagery literacy: resolution tiers, licensing, and provenance

Concept. Commercial imagery literacy: resolution tiers, licensing, and provenance treats location evidence as a quality and uncertainty problem, separating map interpretation from targeting or attribution.

Why it matters. Commercial imagery literacy connects classroom vocabulary to Open-Source and Geospatial Intelligence Integrity practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Commercial imagery literacy: resolution tiers, licensing, and provenance rests on [302, 2026] and [297, 2026]. The most specific cited work observes: It describes NGA's mission of delivering geospatial intelligence, or GEOINT, to support military operations, policymakers, and first responders, spanning imagery analysis, mapping, geodesy, and navigation safety. Use them for fixing what **Commercial imagery literacy: resolution tiers, licensing, and provenance** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. Read **Commercial imagery literacy** against the works cited for this row. [302, 2026] The official "About Us" page of the National Geospatial-Intelligence Agency (NGA), a U.S. Department of Defense and intelligence community organization. It describes NGA's mission of delivering geospatial intelligence, or GEOINT, to support military operations, policymakers, and first responders, spanning imagery analysis, mapping, geodesy, and navigation safety. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Commercial imagery literacy**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this source-quality review and non-sensitive geospatial interpretation topic. The artifact must list the imagery descriptor, the bounded claim about **Commercial imagery literacy**, the resolution caveat, the uncertainty note, the sensitive-site boundary, and the reviewer who checks the interpretation. Shape **Commercial imagery literacy** work as a **location-and-entity evidence ledger** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Commercial imagery literacy**: that a visible feature is enough for a confident geospatial claim.

Transfer task. Reuse the **Commercial imagery literacy** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

25.2.2.5 Lesson 5: Open-source geolocation literacy: resolution, corroboration, and uncertainty

Concept. Open-source geolocation literacy: resolution, corroboration, and uncertainty compares resolution, accuracy, and temporal fitness before drawing a geospatial conclusion from imagery or map products.

Why it matters. Open-source geolocation literacy matters in the **Open-Source and Geospatial Intelligence Integrity** lane because source-quality review and non-sensitive geospatial interpretation evidence must stay separate from judgment; privacy drift is a common failure.

Source support. Open-source geolocation literacy: resolution, corroboration, and uncertainty rests on [302, 2026] and [297, 2026]. The most specific cited work observes: Department of Defense and intelligence community organization. Use them for the claim that **Open-source geolocation literacy: resolution, corroboration, and uncertainty** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of the Director of National Intelligence and Agency, 2024]; [of State, 2024].

Evidence to inspect. Ground **Open-source geolocation literacy** in the evidence the row cites. [302, 2026] The official "About Us" page of the National Geospatial-Intelligence Agency (NGA), a U.S. Department of Defense and intelligence community organization. It describes NGA's mission of delivering geospatial intelligence, or GEOINT, to support military operations, policymakers, and first responders, spanning imagery analysis, mapping, geodesy, and navigation safety. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Open-source geolocation literacy**, build a **requirements matrix with source descriptors, caveats, and collection limits** for this source-quality review and non-sensitive geospatial interpretation topic. The artifact must list the imagery descriptor, the bounded claim about **Open-source geolocation literacy**, the resolution caveat, the uncertainty note, the sensitive-site boundary, and the reviewer who checks the interpretation. Shape **Open-source geolocation literacy** work as a **location-and-entity evidence ledger** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Open-source geolocation literacy**: that a visible feature in imagery is enough for confident attribution without resolution, timing, and provenance caveats.

Transfer task. Apply this module's safe boundary for **Open-source geolocation literacy** to another artifact while keeping source-quality review and non-sensitive geospatial interpretation and reviewer ownership explicit.

25.2.3 Imagery Intelligence (IMINT) worked safe example: synthetic inputs, evidence, and review

Worked example: a synthetic public-resilience team checks whether open data supports a non-sensitive evacuation-route map. [253, 2026]; [269, 2026].

Triangulation anchors. In module 16's worked-example section, directly verified anchors for the **Open-Source and Geospatial Intelligence Integrity** lane include [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]; [Agency, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **geospatial and financial intelligence uncertainty**. Learners use a **location-and-entity evidence ledger** and keep this boundary visible: No facility targeting, pattern-of-life inference, evasion advice, or attribution certainty beyond evidence.

Frame. The classroom question centers on **Imagery modality literacy: resolution, scale, and sensor-fit**. Excluded actions stay explicit, and the **Requirements-to-Evidence Lens** planning question is: What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit?

Inputs. For the **Imagery modality literacy: resolution, scale, and sensor-fit** scenario, use public road data, public weather notices, synthetic change examples, and instructor-provided metadata. The Requirements-to-Evidence Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Imagery modality literacy: resolution, scale, and sensor-fit**, students record provenance, test recency, compare independent sources, mark uncertainty, and remove unnecessary identity data. Pause whenever an inference about Imagery modality literacy: resolution, scale, and sensor-fit appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Imagery modality literacy: resolution, scale, and sensor-fit** classroom scenario; unit artifact = location-and-entity evidence ledger; evidence = allowed inputs; method = source-quality review and non-sensitive geospatial interpretation; output = a source-quality matrix and annotated map note with caveats and no tracking or targeting content; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Imagery modality literacy: resolution, scale, and sensor-fit** as "Requirements-to-Evidence Lens confirms it" is not enough. The revision ties the claim to source-quality review and non-sensitive geospatial interpretation, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Imagery modality literacy: resolution, scale, and sensor-fit** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

25.2.4 Imagery Intelligence (IMINT) practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Requirements-to-Evidence Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**.

Triangulation anchors. In module 16's practice-sequence section, directly verified anchors for the **Open-Source and Geospatial Intelligence Integrity** lane include [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]; [Agency, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Imagery modality literacy: resolution, scale, and sensor-fit, Imagery collection-platform literacy: resolution and revisit tradeoffs, Photo-interpretation literacy: resolution, uncertainty, and scale; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Open-Source and Geospatial Intelligence Integrity** lane.
2. Frame	Answer the lens question: What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Imagery modality literacy: resolution, scale, and sensor-fit: requirements matrix with source descriptors, caveats, and collection limits.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the location-and-entity evidence ledger fields for Imagery modality literacy: resolution, scale, and sensor-fit.	Unit profile note.	Evidence artifacts include geospatial quality note, temporal caveat.
4. Challenge	Test the misconception that a visible feature is enough for a confident geospatial claim.	Failure-mode note.	The artifact applies the key distinction: separate discovery from collection expansion, and map or media interpretation from targeting.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

25.2.4.1 Imagery Intelligence (IMINT) instructor notes: source reasoning, review points, and studio focus

Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**. [253, 2026]; [269, 2026].

25.2.4.2 Imagery Intelligence (IMINT) extension exercise: peer validation and refresh trigger review

Evidence anchor. Section 25; [253, 2026].

Have learners swap artifacts and apply the **Requirements-to-Evidence Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**.

25.2.5 Imagery Intelligence (IMINT) knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 25; [253, 2026].

1. Explain how **Imagery modality literacy: resolution, scale, and sensor-fit** is defined here; name the source descriptor that supports the definition.
2. Contrast **Imagery modality literacy: resolution, scale, and sensor-fit** with **Imagery collection-platform literacy: resolution and revisit tradeoffs** using the **Requirements-to-Evidence Lens** artifact fields.
3. Identify one failure mode from the **Open-Source and Geospatial Intelligence Integrity** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which source is available but not reliable enough for the claim?
5. Correct this misconception: that a visible feature is enough for a confident geospatial claim.

25.2.5.1 Imagery Intelligence (IMINT) answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Imagery modality literacy: resolution, scale, and sensor-fit** without source evidence, uncertainty, or a safe transfer task.

25.3 Imagery Intelligence (IMINT) assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 25; [253, 2026].

25.3.1 Imagery Intelligence (IMINT) evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 25; [253, 2026].

25.3.2 Imagery Intelligence (IMINT) transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 25; [253, 2026].

25.3.2.1 Imagery Intelligence (IMINT) lineage and source tradition: profile, concepts, and first anchors This sits in the **Open-Source and Geospatial Intelligence Integrity** lineage: public-source discovery converted into accountable intelligence through provenance, corroboration, minimization, and relevance tests. [253, 2026]; [269, 2026].

25.3.2.2 Imagery Intelligence (IMINT) working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 25; [253, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**, with provenance and reviewability throughout.

25.3.2.3 Imagery Intelligence (IMINT) knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [253, 2026]; [269, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

25.3.2.4 Imagery Intelligence (IMINT) transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 25; [253, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**.
- **Evidence contract:** keep the **Open-Source and Geospatial Intelligence Integrity** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

25.3.2.5 Imagery Intelligence (IMINT) profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 25; [253, 2026].

The matched profile emphasizes public-source discovery converted into accountable intelligence through provenance, corroboration, minimization, and relevance tests. The method stack is source triage, provenance capture, corroboration matrix, recency audit, geospatial context review, and confidence calibration; the local topic cluster is **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**.

25.3.3 Imagery Intelligence (IMINT) evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 25; [253, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Open-Source and Geospatial Intelligence Integrity** profile tells reviewers what evidence is strong enough for the module artifact built around **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**.

25.3.3.1 Imagery Intelligence (IMINT) guide source spine: inherited keys and local citation roles Primary guide citations: [253, 2026]; [269, 2026]; [270, 2026]; [275, 2026]; [276, 2026]; [283, 2026]; [286, 2026]; [293, 2026]; [295, 2026]; [302, 2026]; [297, 2026]; [309, 2026]; [310, 2026]; [300, 2026].

25.3.3.2 Imagery Intelligence (IMINT) verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [253, 2026]; [269, 2026].

Tier	What counts	How it is used
Source guide	[253, 2026]; [269, 2026]; [270, 2026]; [275, 2026]; [276, 2026]; [283, 2026]; [286, 2026]; [293, 2026]; [295, 2026]; [302, 2026]; [297, 2026]; [309, 2026]; [310, 2026]; [300, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 16's source-canon section, directly verified anchors for the **Open-Source and Geospatial Intelligence Integrity** lane include [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]; [Agency, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs** and [253, 2026]; [269, 2026], but only directly verified source URLs are encoded as citations.

25.3.3.3 Imagery Intelligence (IMINT) intelligence practice lens: evidence artifact and safety check Practice lens: **Requirements-to-Evidence Lens** for **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**. [253, 2026]; [269, 2026].

Planning question: What accountable requirement justifies the evidence, and which source discipline is the least intrusive fit?

Evidence artifact: requirements matrix with source descriptors, caveats, and collection limits.

Validation rule: show priority, authority, minimization, corroboration, and source quality before any claim is reused. Applied to **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**.

Handoff contract: deliver metadata-rich evidence packets, not unscoped data piles or implicit targeting requests.

Safety check: exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure.

25.3.3.4 Imagery Intelligence (IMINT) runtime-to-reader map: generated sections and verifier surfaces **Evidence anchor.** Section 25; [253, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	16.99	16.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Imagery Intelligence (IMINT) to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Bounded autonomy, procurement, incident-response, and assurance studio	16.101	16.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Imagery Intelligence (IMINT)	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Model-card, recoverability, retention, and learner-support evidence package	16.102	16.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Imagery Intelligence (IMINT)	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Imagery modality literacy: resolution, scale, and sensor-fit	16.1	16.1 source title transformed into safe curriculum treatment; original: Types: Optical, SAR, Infrared, Hyperspectral, Multispectral	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Imagery collection-platform literacy: resolution and revisit tradeoffs	16.2	16.2 source title transformed into safe curriculum treatment; original: Collection Platforms: Satellites, UAVs, Aircraft, Ground-Based	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Photo-interpretation literacy: resolution, uncertainty, and scale	16.3	16.3 source title transformed into safe curriculum treatment; original: Photo Interpretation and All-Source Imagery Analysis	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Commercial imagery literacy: resolution tiers, licensing, and provenance	16.4	16.4 source title transformed into safe curriculum treatment; original: Commercial IMINT and the Democratization of Space-Based Reconnaissance	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Open-source geolocation literacy: resolution, corroboration, and uncertainty	16.5	16.5 source title transformed into safe curriculum treatment; original: Open-Source Geolocation Methods: Bellingcat Methodology	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

25.3.3.5 Imagery Intelligence (IMINT) reusable subsection contract: topic rows, artifacts, and safety duties **Evidence anchor.** Section 25; [253, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Imagery modality literacy: resolution, scale, and sensor-fit	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Imagery collection-platform literacy: resolution and revisit tradeoffs	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Photo-interpretation literacy: resolution, uncertainty, and scale	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Commercial imagery literacy: resolution tiers, licensing, and provenance	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Open-source geolocation literacy: resolution, corroboration, and uncertainty	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

25.3.3.6 Imagery Intelligence (IMINT) annotated source ledger: real titles and local contribution Each source cited by this **Open-Source and Geospatial Intelligence Integrity** module is paired below with its real title and a one-line note on what it contributes to **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**.

Source	Cited work	What it contributes	Status
[253, 2026]	Common European Data Spaces	This is an official European Commission webpage describing the Common European Data Spaces initiative, part of the EU strategy to create interconnected, trustworthy data-sharing environments across strategic sectors. It explains that data spaces let organizations and individuals share data while retaining control, guided by principles of open participation, privacy protection, and fair access rules.	verified source-guide

Source	Cited work	What it contributes	Status
[269, 2026]	Data on the Web Best Practices	A W3C Recommendation, "Data on the Web Best Practices," published January 31, 2017 by the Data on the Web Best Practices Working Group. It offers 35 best practices for publishing and consuming data on the Web, covering metadata, licensing and provenance, data quality, dataset versioning, persistent URIs, machine-readable formats, vocabulary reuse, access methods, preservation, and feedback.	verified source-guide
[270, 2026]	NIST Big Data Interoperability Framework	NIST Special Publication 1500-1 (revised edition by Chang and Grady) establishes foundational terminology and consensus definitions for Big Data through the NIST Big Data Public Working Group. The volume defines Big Data characteristics, taxonomy, and a reference architecture assigning roles to Application Providers, Data Consumers, Data Providers, and System Orchestrators.	verified source-guide
[275, 2026]	Fact Sheet: New Rule on the Accessibility of Web Content and Mobile Apps Provided by State and Local Governments	A US Department of Justice fact sheet explaining the 2024 ADA Title II rule requiring state and local governments to make their web content and mobile apps accessible. It establishes WCAG 2.1 Level AA as the technical standard, applies to entities such as schools, courts, libraries, and transit agencies, and sets compliance deadlines of April 2027 for larger jurisdictions and April 2028 for smaller ones.	verified source-guide
[276, 2026]	What is a Data Protection Impact Assessment and When Is This Mandatory?	A European Data Protection Board FAQ page, part of its data protection guide for small businesses, explaining Data Protection Impact Assessments (DPIAs) and when they are mandatory. It describes a DPIA as a written assessment of the impact of a planned processing operation, required when processing poses high risks to individuals' rights.	verified source-guide
[283, 2026]	Recommendation of the Council on Open Government	An OECD legal instrument document reproducing the Recommendation of the Council on Open Government (OECD/LEGAL/0438), adopted on 14 December 2017. It defines open government as a culture of governance promoting transparency, integrity, accountability, and stakeholder participation in support of democracy and inclusive growth.	verified source-guide
[286, 2026]	Model Cards for Model Reporting	The arXiv abstract for "Model Cards for Model Reporting" (2018) by Mitchell, Wu, Zaldivar, and colleagues, which introduces a framework for transparent documentation of machine learning models. Model cards are short accompanying documents that report a model's benchmarked performance across varied conditions, including different cultural, demographic, and phenotypic groups, along with intended use, evaluation methodology, and deployment considerations.	verified source-guide

Source	Cited work	What it contributes	Status
[293, 2026]	Inventory of NARA Artificial Intelligence (AI) Use Cases	The National Archives and Records Administration (NARA) official inventory of its artificial intelligence use cases, documenting 14 projects across deployed, pilot, and planned stages. Deployed efforts include workplace productivity tools, automated tagging for museum experiences, and historical record retrieval, while pilots cover PII detection and redaction, semantic search, and metadata generation, and planned work targets FOIA processing and public search.	verified source-guide
[295, 2026]	M-25-22: Driving Efficient Acquisition of Artificial Intelligence in Government	OMB Memorandum M-25-22 (April 3, 2025), Driving Efficient Acquisition of Artificial Intelligence in Government, issued under Executive Order 13960 and related directives. It provides guidance to federal agencies for acquiring effective and trustworthy AI in a timely, cost-effective manner, and rescinds and replaces earlier memorandum M-24-18.	verified source-guide
[302, 2026]	National Geospatial-Intelligence Agency About Us	The official "About Us" page of the National Geospatial-Intelligence Agency (NGA), a U.S. Department of Defense and intelligence community organization. It describes NGA's mission of delivering geospatial intelligence, or GEOINT, to support military operations, policymakers, and first responders, spanning imagery analysis, mapping, geodesy, and navigation safety.	verified source-guide
[297, 2026]	Intelligence Community Directive 203: Analytic Standards	Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products.	original source-guide
[309, 2026]	STIX Version 2.1	An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection.	verified source-guide
[310, 2026]	TAXII Version 2.1	The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe).	verified source-guide
[300, 2026]	MITRE ATLAS	MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy.	original source-guide

Where this sits. This module's overview is Section 25; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

25.3.4 Imagery Intelligence (IMINT) governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 25; [253, 2026].

25.3.5 Imagery Intelligence (IMINT) analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 16's governance-boundary section, directly verified anchors for the **Open-Source and Geospatial Intelligence Integrity** lane include [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]; [Agency, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Research lane: **Open-Source and Geospatial Intelligence Integrity** for **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**. [253, 2026]; [269, 2026].
Curriculum topic spine: Imagery modality literacy: resolution, scale, and sensor-fit, **Imagery collection-platform literacy: resolution and revisit tradeoffs**, **Photo-interpretation literacy: resolution, uncertainty, and scale**. **Verified anchor cluster:** [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]; [Agency, 2026b]; [for Standardization, 2013]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015].
Conceptual depth: public-source discovery converted into accountable intelligence through provenance, corroboration, minimization, and relevance tests.
Method stack: source triage, provenance capture, corroboration matrix, recency audit, geospatial context review, and confidence calibration.
Composability contract: collection notes, source metadata, transformations, caveats, and analytic judgments remain separately exportable.
Known failure modes: privacy drift, stale data, context collapse, platform bias, over-collection, and mistaking availability for reliability.
Defensive boundary: OSINT work uses lawful public, owned-lab, or explicitly approved sources and avoids doxxing, harassment, live tracking, or operational targeting. Applied to **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**.

Anchor	Why it matters here
[of the Director of National Intelligence and Agency, 2024]	Official IC OSINT strategy for professionalizing OSINT, integrated collection management, open-source sharing, innovation, and tradecraft. Checked as of 2026-05-21; role: curriculum_anchor.
[of State, 2024]	Official strategy source for lawful OSINT governance, discovery, validation, and dissemination. Checked as of 2026-05-21; role: curriculum_anchor.
[Agency, 2026c]	Official NGA strategy anchor for GEOINT readiness, warning, partnership resilience, resource stewardship, and AI integration. Checked as of 2026-05-21; role: curriculum_anchor.
[Agency, 2026b]	Official NGA source on GEOINT AI, data quality, model performance, interoperability, analyst interaction, and standards leadership. Checked as of 2026-05-21; role: curriculum_anchor.
[for Standardization, 2013]	International geospatial data-quality standard for completeness, logical consistency, positional accuracy, temporal quality, and usability framing. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026d]	Official sourcing directive for traceability, citations, source descriptors, and source summaries. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2015]	Official ODNI analytic tradecraft standards directive. Checked as of 2026-05-21; role: source_quality_anchor.

25.3.5.1 Imagery Intelligence (IMINT) evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **Open-Source and Geospatial Intelligence Integrity** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [253, 2026]; [269, 2026].

25.3.6 Imagery Intelligence (IMINT) agentic boundary: assist, approve, block, and record

Evidence anchor. Section 25; [253, 2026].
AGEINT translation is bounded by the **Open-Source and Geospatial Intelligence Integrity** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**.

25.3.6.1 Imagery Intelligence (IMINT) permitted defensive utility: curriculum uses and safe outputs

Evidence anchor. Section 25; [253, 2026].
The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**.

25.3.6.2 Imagery Intelligence (IMINT) excluded operational boundary: blocked actions and stop rules

Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [253, 2026]; [269, 2026] and **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

25.3.7 Imagery Intelligence (IMINT) governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 25; [253, 2026].
Governance is practiced as a gate on the **Open-Source and Geospatial Intelligence Integrity** lane. Learners use the **Requirements-to-Evidence Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**.

25.3.7.1 Imagery Intelligence (IMINT) governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [253, 2026]; [269, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Open-Source and Geospatial Intelligence Integrity** failure modes and the **Requirements-to-Evidence Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

25.3.7.2 Imagery Intelligence (IMINT) evidence package handoff: appendices, records, and reuse Evidence anchor. Section 25; [253, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Requirements-to-Evidence Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**.

25.3.7.3 Imagery Intelligence (IMINT) current-source assurance: verified anchors and local artifact fit The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**. [253, 2026]; [269, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_ic_osint_strategy` for **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**?	The INT of First Resort: The IC OSINT Strategy 2024-2026; lane `osint_geoint`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official IC OSINT strategy for professionalizing OSINT, integrated collection management, open-source sharing, innovation, and tradecraft.
What does the module inherit from `official_state_osint_strategy` for **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**?	Open Source Intelligence Strategy; lane `osint_geoint`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official strategy source for lawful OSINT governance, discovery, validation, and dissemination.
What does the module inherit from `official_nga_strategy` for **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**?	NGA Strategy; lane `osint_geoint`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official NGA strategy anchor for GEOINT readiness, warning, partnership resilience, resource stewardship, and AI integration.
What does the module inherit from `official_nga_geoint_ai` for **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**?	GEOINT Artificial Intelligence; lane `osint_geoint`; checked 2026-05-21.	requirements matrix with source descriptors, caveats, and collection limits; Official NGA source on GEOINT AI, data quality, model performance, interoperability, analyst interaction, and standards leadership.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 25; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

25.3.8 Imagery Intelligence (IMINT) assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 25; [253, 2026].

25.3.9 Imagery Intelligence (IMINT) assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 25; [253, 2026].

25.3.9.1 Imagery Intelligence (IMINT) capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs** and [253, 2026]; [269, 2026].

25.3.9.2 Imagery Intelligence (IMINT) instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs** and [253, 2026]; [269, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

25.3.9.3 Imagery Intelligence (IMINT) assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Imagery modality literacy: resolution, scale, and sensor-fit	Completed **requirements matrix with source descriptors, caveats, and collection limits** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Imagery collection-platform literacy: resolution and revisit tradeoffs	Completed **requirements matrix with source descriptors, caveats, and collection limits** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Photo-interpretation literacy: resolution, uncertainty, and scale	Completed **requirements matrix with source descriptors, caveats, and collection limits** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

25.3.10 Imagery Intelligence (IMINT) refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [253, 2026]; [269, 2026] and **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**.

25.3.10.1 Imagery Intelligence (IMINT) refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**. The local signals begin with [253, 2026]; [269, 2026].

25.3.10.2 Imagery Intelligence (IMINT) claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**, and the source spine for these checks begins with [253, 2026]; [269, 2026].

25.3.11 Imagery Intelligence (IMINT) reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [253, 2026]; [269, 2026].

Triangulation anchors. In module 16's review-checklist section, directly verified anchors for the **Open-Source and Geospatial Intelligence Integrity** lane include [of the Director of National Intelligence and Agency, 2024]; [of State, 2024]; [Agency, 2026c]; [Agency, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs**. [253, 2026]; [269, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

25.3.12 Imagery Intelligence (IMINT) learning-path links: module map, overview, and curriculum atlas

These links keep **Imagery modality literacy: resolution, scale, and sensor-fit; Imagery collection-platform literacy: resolution and revisit tradeoffs** paired with the orientation atlas, the parent unit, and the previous and next modules, so a reader can trace which claims and caveats are inherited rather than re-derived here. Anchored at [253, 2026]; [269, 2026].

Section 2, Section 24, Section 26

26 Financial Intelligence (FININT)

26.0.1 Financial Intelligence (FININT) figures and course links: visual evidence, source flow, and navigation

The module uses Figure 63 and Figure 58 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 24, Section 25, Section 27.
This module teaches the **Financial Intelligence and Economic-Security Due Diligence** lane through a bounded, source-backed coursebook chapter. [251, 2026]; [252, 2026].

26.1 Financial Intelligence and Economic-Security Due Diligence frame for Financial Intelligence (FININT): source context, topic focus, and reader task

Evidence anchor. Section 26; [251, 2026].

26.1.1 Financial Intelligence (FININT) orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 26; [251, 2026].

26.1.2 Financial Intelligence (FININT) conceptual primer: source context, core model, and reader task

This chapter teaches FININT and economic-security analysis as lawful due diligence: signals are interpreted through official lists, typology context, beneficial-ownership uncertainty, and compliance boundaries. The chapter uses **Economic-Security Due-Diligence Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**.
The central distinction is to separate compliance-oriented risk analysis from evasion, attribution certainty, or targeting. Core topics include **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries; Non-state actor indicator review with attribution caution and governance boundaries**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Network, 2026a]; [Network, 2026b]; [of Foreign Assets Control, 2026]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [251, 2026]; [252, 2026].
Learners move from vocabulary and the **Economic-Security Due-Diligence Lens** distinction through topic lessons on **FININT Foundations: Collection, Analysis, Reporting** with evidence and misconception checks, then assemble an **economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary** with safety and rights gates.

26.1.3 Financial Intelligence (FININT) learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 26; [251, 2026].

- Connect **FININT Foundations: Collection, Analysis, Reporting and Financial due-diligence typology exercise using synthetic records and compliance boundaries** to **Financial Intelligence and Economic-Security Due Diligence** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build an **economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate compliance-oriented risk analysis from evasion, attribution certainty, or targeting; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as evasion playbooks, threshold gaming, overconfident attribution, stale sanctions data, unverified beneficial ownership, and confusing compliance screening with intelligence certainty, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: FININT and economic-security examples remain compliance, policy, and resilience oriented; they do not explain how to launder funds, evade sanctions, bypass export controls, or target real firms.

26.1.4 Financial Intelligence (FININT) core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 26; [251, 2026].

Term	Working definition
Typology	a recurring pattern used to recognize financial-crime or sanctions-risk signals
Sanctions program	the legal and policy structure behind a restricted-party or country measure
Beneficial ownership	the natural-person control or ownership question behind an entity
Red flag	an indicator that triggers review rather than a standalone conclusion
Compliance boundary	the line between lawful screening or resilience analysis and prohibited evasion advice
FININT Foundations: Collection, Analysis,…	Key terms: FININT, Foundations, Collection.
Financial due-diligence typology exercise using…	Key terms: Financial, due, diligence.

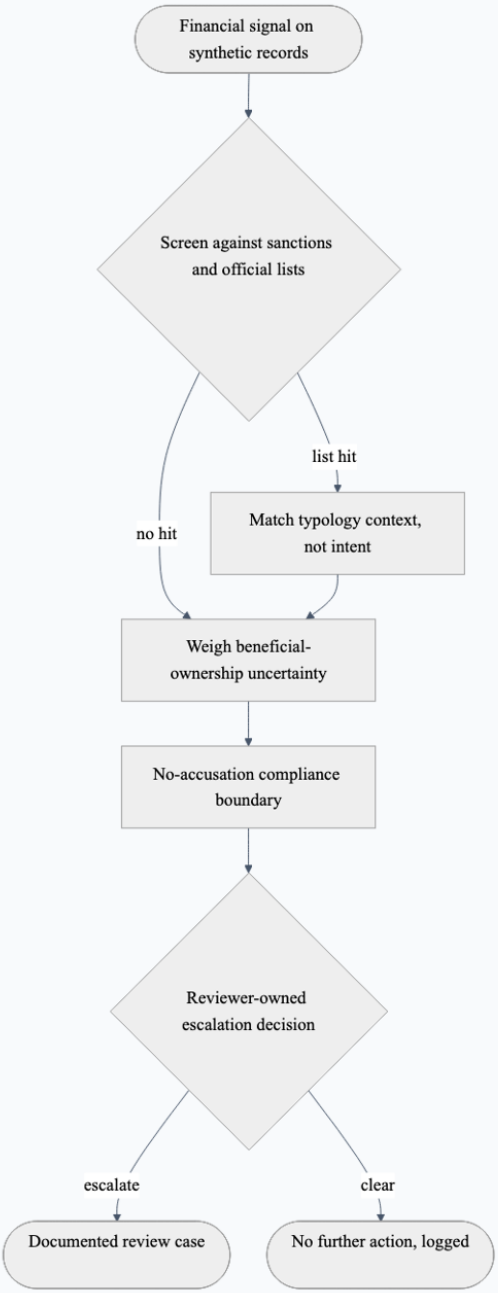


Figure 63: This diagram shows the lawful due-diligence workflow where a financial signal is screened against official lists and typology context, with uncertainty preserved so a typology match triggers review rather than an accusation of intent. It is anchored to the imagery and financial intelligence / financial intelligence finint section; use it to inspect Financial signal on synthetic records, Match typology context, not intent, Weigh beneficial-ownership uncertainty, and No-accusation compliance boundary while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

26.2 Economic-Security Due-Diligence Lens path for Financial Intelligence (FININT): lesson cluster, safe artifact, and review

Evidence anchor. Section 26; [251, 2026].

26.2.1 Financial Intelligence (FININT) practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 26; [251, 2026].

26.2.2 Financial Intelligence (FININT) topic lessons: source-backed concepts and transfer tasks

This module builds FININT and economic-security analysis as lawful due diligence: signals are interpreted through official lists, typology context, beneficial-ownership uncertainty, and compliance boundaries. The sequence opens with **FININT Foundations: Collection, Analysis, Reporting**, **Financial due-diligence typology exercise using synthetic records and compliance boundaries**, **Non-state actor indicator review with attribution caution and governance boundaries** and applies the **Economic-Security Due-Diligence Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 58; module overview Section 26; curriculum atlas Section 2.

Triangulation anchors. In module 17's topic-lessons section, directly verified anchors for the **Financial Intelligence and Economic-Security Due Diligence** lane include [Network, 2026a]; [Network, 2026b]; [of Foreign Assets Control, 2026]; [of Foreign Assets Control, 2019]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

26.2.2.1 Lesson 1: FININT Foundations: Collection, Analysis, Reporting

Concept. **FININT Foundations: Collection, Analysis, Reporting** reads financial intelligence as due-diligence evidence that triggers review rather than proof of intent or guilt.

Why it matters. Analysts use **FININT Foundations** to separate compliance-oriented risk analysis from evasion, attribution certainty, or targeting. A defensible treatment names the judgment it enables for defensive due diligence and uncertainty-preserving FININT review, the proof limit that evasion playbooks would otherwise hide, and the reviewer accountable for challenge.

Source support. FININT Foundations: Collection, Analysis, Reporting rests on [079, 2026] and [080, 2026]. The most specific cited work observes: The article describes the U.S. Use them for pinning down the scope of **FININT Foundations: Collection, Analysis, Reporting**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Network, 2026a]; [Network, 2026b].

Evidence to inspect. For **FININT Foundations**, work from the cited evidence behind this row. [079, 2026] The Wikipedia article on financial intelligence (FININT), defined as gathering information about the financial affairs of entities of interest to understand their nature, capabilities, and intentions. It outlines two core components: collection, in which Financial Intelligence Units gather transaction data and suspicious activity reports from banks, and analysis, in which specialists use data mining to detect tax evasion, money laundering, and terrorist financing. [080, 2026] A Wikipedia article on financial intelligence (FININT), the gathering and analysis of information about financial transactions to detect illicit activity such as money laundering, tax evasion, and terrorist financing. It distinguishes two core functions: collection of raw transaction data and suspicious activity reports by government financial intelligence units, and analysis using data-matching techniques to identify suspicious patterns. The article describes the U.S. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **FININT Foundations**, build a **economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary** for this defensive due diligence and uncertainty-preserving FININT topic. The artifact must name the source descriptor, the bounded claim about **FININT Foundations**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **FININT Foundations** work as a **location-and-entity evidence ledger** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that FININT Foundations: Collection, Analysis, Reporting establishes intent without reviewing alternative explanations.

Transfer task. Transfer **FININT Foundations** to a second module by preserving defensive due diligence and uncertainty-preserving FININT, changing the source evidence, and naming a new reviewer.

26.2.2.2 Lesson 2: Financial due-diligence typology exercise using synthetic records and compliance boundaries

Concept. **Financial due-diligence typology exercise using synthetic records and compliance boundaries** reads financial intelligence as due-diligence evidence that triggers review rather than proof of intent or guilt.

Why it matters. Analysts use **Financial due-diligence typology exercise** to separate compliance-oriented risk analysis from evasion, attribution certainty, or targeting. A defensible treatment names the judgment it enables for defensive due diligence and uncertainty-preserving FININT review, the proof limit that treating typology match as proof of intent would otherwise hide, and the reviewer accountable for challenge.

Source support. Financial due-diligence typology exercise using synthetic records and compliance boundaries rests on [079, 2026]. The closest source to this row notes: It outlines two core components: collection, in which Financial Intelligence Units gather transaction data and suspicious activity reports from banks, and analysis, in which specialists use data mining to detect tax evasion, money laundering, and terrorist financing. Use it for pinning down the scope of **Financial due-diligence typology exercise using synthetic records and compliance boundaries**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Network, 2026a]; [Network, 2026b].

Evidence to inspect. Ground **Financial due-diligence typology exercise** in the evidence the row cites. [079, 2026] The Wikipedia article on financial intelligence (FININT), defined as gathering information about the financial affairs of entities of interest to understand their nature, capabilities, and intentions. It outlines two core components: collection, in which Financial Intelligence Units gather transaction data and suspicious activity reports from banks, and analysis, in which specialists use data mining to detect tax evasion, money laundering, and terrorist financing. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Financial due-diligence typology exercise**, build a **economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary** for this defensive due diligence and uncertainty-preserving FININT topic. The artifact must note the typology descriptor, the bounded claim about **Financial due-diligence typology exercise using**, the intent caveat, the uncertainty threshold, the no-accusation boundary, and the reviewer who owns escalation. Shape **Financial due-diligence typology exercise** work as a **location-and-entity evidence ledger** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Financial due-diligence typology exercise**: that a typology or pattern match is proof of intent rather than a flag requiring corroboration and alternative explanations.

Transfer task. Apply this module's safe boundary for **Financial due-diligence typology exercise** to another artifact while keeping defensive due diligence and uncertainty-preserving FININT and reviewer ownership explicit.

26.2.2.3 Lesson 3: Non-state actor indicator review with attribution caution and governance boundaries

Concept. **Non-state actor indicator review with attribution caution and governance boundaries** uses attribution indicators cautiously by separating technical similarity, context, confidence, and geopolitical inference.

Why it matters. Non-state actor indicator review matters in the **Financial Intelligence and Economic-Security Due Diligence** lane because defensive due diligence and uncertainty-preserving FININT evidence must stay separate from judgment; evasion playbooks is a common failure.

Source support. Non-state actor indicator review with attribution caution and governance boundaries rests on [079, 2026]. The lead source's own note reads: The Wikipedia article on financial intelligence (FININT), defined as gathering information about the financial affairs of entities of interest to understand their nature, capabilities, and intentions. Use it for the claim that **Non-state actor indicator review with attribution caution and governance boundaries** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Network, 2026a]; [Network, 2026b].

Evidence to inspect. For **Non-state actor indicator review**, work from the cited evidence behind this row. [079, 2026] The Wikipedia article on financial intelligence (FININT), defined as gathering information about the financial affairs of entities of interest to understand their nature, capabilities, and intentions. It outlines two core components: collection, in which Financial Intelligence Units gather transaction data and suspicious activity reports from banks, and analysis, in which specialists use data mining to detect tax evasion, money laundering, and terrorist financing. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Non-state actor indicator review**, build a **economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary** for this defensive due diligence and uncertainty-preserving FININT topic. The artifact must name the actor descriptor, the bounded claim about **state actor indicator review with**, the attribution caveat, the uncertainty note, the non-targeting boundary, and the reviewer who approves the assessment. Shape **Non-state actor indicator review** work as a **location-and-entity evidence ledger** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that lacking a state sponsor places an actor outside the reach of governance, accountability, and applicable rules.

Transfer task. Transfer **Non-state actor indicator review** from this module to a second motif by preserving defensive due diligence and uncertainty-preserving FININT, replacing action with audit, and naming the blocked use.

26.2.2.4 Lesson 4: The SWIFT System and Intelligence Collection

Concept. The SWIFT System and Intelligence Collection applies SWIFT, System, Collection within Financial Intelligence and Economic-Security Due Diligence: learners use separate compliance-oriented risk analysis from evasion, attribution certainty, or targeting and defensive due diligence and uncertainty-preserving FININT evidence before any judgment moves forward.

Why it matters. The SWIFT System matters in the **Financial Intelligence and Economic-Security Due Diligence** lane because defensive due diligence and uncertainty-preserving FININT evidence must stay separate from judgment; evasion playbooks is a common failure.

Source support. The SWIFT System and Intelligence Collection rests on [079, 2026]. The closest source to this row notes: It outlines two core components: collection, in which Financial Intelligence Units gather transaction data and suspicious activity reports from banks, and analysis, in which specialists use data mining to detect tax evasion, money laundering, and terrorist financing. Use it for pinning down the scope of **The SWIFT System and Intelligence Collection**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Network, 2026a]; [Network, 2026b].

Evidence to inspect. Ground **The SWIFT System** in the evidence the row cites. [079, 2026] The Wikipedia article on financial intelligence (FININT), defined as gathering information about the financial affairs of entities of interest to understand their nature, capabilities, and intentions. It outlines two core components: collection, in which Financial Intelligence Units gather transaction data and suspicious activity reports from banks, and analysis, in which specialists use data mining to detect tax evasion, money laundering, and terrorist financing. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **The SWIFT System**, build a **economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary** for this defensive due diligence and uncertainty-preserving FININT topic. The artifact must name the source descriptor, the bounded claim about **SWIFT System and Intelligence Collection**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **The SWIFT System** work as a **location-and-entity evidence ledger** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that The SWIFT System and Intelligence Collection is optional whenever separate compliance-oriented risk analysis from evasion, attribution certainty, or targeting feels inconvenient.

Transfer task. Transfer **The SWIFT System** to a second module by preserving defensive due diligence and uncertainty-preserving FININT, changing the source evidence, and naming a new reviewer.

26.2.2.5 Lesson 5: Cryptocurrency as Covert Finance: Monero, Mixers, Bridges

Concept. Cryptocurrency as Covert Finance: Monero, Mixers, Bridges applies Cryptocurrency, Covert, Finance within Financial Intelligence and Economic-Security Due Diligence: learners use separate compliance-oriented risk analysis from evasion, attribution certainty, or targeting and defensive due diligence and uncertainty-preserving FININT evidence before any judgment moves forward.

Why it matters. Cryptocurrency as Covert Finance connects classroom vocabulary to Financial Intelligence and Economic-Security Due Diligence practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Cryptocurrency as Covert Finance: Monero, Mixers, Bridges rests on [302, 2026] and [297, 2026]. Its anchor reference records: It describes NGA's mission of delivering geospatial intelligence, or GEOINT, to support military operations, policymakers, and first responders, spanning imagery analysis, mapping, geodesy, and navigation safety. Use them for fixing what **Cryptocurrency as Covert Finance: Monero, Mixers, Bridges** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Network, 2026a]; [Network, 2026b].

Evidence to inspect. For **Cryptocurrency as Covert Finance**, reason from the sources cited in this row. [302, 2026] The official "About Us" page of the National Geospatial-Intelligence Agency (NGA), a U.S. Department of Defense and intelligence community organization. It describes NGA's mission of delivering geospatial intelligence, or GEOINT, to support military operations, policymakers, and first responders, spanning imagery analysis, mapping, geodesy, and navigation safety. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Cryptocurrency as Covert Finance**, build a **economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary** for this defensive due diligence and uncertainty-preserving FININT topic. The artifact must name the source descriptor, the bounded claim about **Cryptocurrency as Covert Finance**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Cryptocurrency as Covert Finance** work as a **location-and-entity evidence ledger** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that Cryptocurrency as Covert Finance: Monero, Mixers, Bridges establishes intent without reviewing alternative explanations.

Transfer task. Transfer **Cryptocurrency as Covert Finance** to a second module by preserving defensive due diligence and uncertainty-preserving FININT, changing the source evidence, and naming a new reviewer.

26.2.2.6 Lesson 6: Economic Warfare and FININT as a Strategic Tool

Concept. Economic Warfare and FININT as a Strategic Tool reads financial intelligence as due-diligence evidence that triggers review rather than proof of intent or guilt.

Why it matters. Without explicit treatment of **Economic Warfare**, evasion playbooks undermines defensive due diligence and uncertainty-preserving FININT review; the lesson builds the habit to separate compliance-oriented risk analysis from evasion, attribution certainty, or targeting.

Source support. Economic Warfare and FININT as a Strategic Tool rests on [081, 2026]. The lead source's own note reads: The Citizendium 'Financial intelligence' article was never written; the page is empty. Use it for the working definition that **Economic Warfare and FININT as a Strategic Tool** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Network, 2026a]; [Network, 2026b].

Evidence to inspect. For **Economic Warfare**, reason from the sources cited in this row. [081, 2026] The Citizendium 'Financial intelligence' article was never written; the page is empty. Use an authoritative alternative source for financial intelligence definitions. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Economic Warfare**, build a **economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary** for this defensive due diligence and uncertainty-preserving FININT topic. The artifact must name the source descriptor, the bounded claim about **Economic Warfare and FININT as**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Economic Warfare** work as a **location-and-entity evidence ledger** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that Economic Warfare and FININT as a Strategic Tool replaces human review whenever evidence looks plausible.

Transfer task. Transfer **Economic Warfare** to a second module by preserving defensive due diligence and uncertainty-preserving FININT, changing the source evidence, and naming a new reviewer.

26.2.2.7 Lesson 7: Money Laundering Detection: Financial due-diligence typology exercise using synthetic records and compliance boundaries

Concept. Money Laundering Detection: Financial due-diligence typology exercise using synthetic records and compliance boundaries uses typologies to structure review of transactional patterns, source quality, and escalation thresholds—not investigative targeting.

Why it matters. Money Laundering Detection matters in the **Financial Intelligence and Economic-Security Due Diligence** lane because defensive due diligence and uncertainty-preserving FININT evidence must stay separate from judgment; treating typology match as proof of intent is a common failure.

Source support. Money Laundering Detection: Financial due-diligence typology exercise using synthetic records and compliance boundaries rests on [080, 2026]. The lead source's own note reads: A Wikipedia article on financial intelligence (FININT), the gathering and analysis of information about financial transactions to detect illicit activity such as money laundering, tax evasion, and terrorist financing. Use it for the working definition that **Money Laundering Detection: Financial due-diligence typology exercise using synthetic records and compliance boundaries** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Network, 2026a]; [Network, 2026b].

Evidence to inspect. Read **Money Laundering Detection** against the works cited for this row. [080, 2026] A Wikipedia article on financial intelligence (FININT), the gathering and analysis of information about financial transactions to detect illicit activity such as money laundering, tax evasion, and terrorist financing. It distinguishes two core functions: collection of raw transaction data and suspicious activity reports by government financial intelligence units, and analysis using data-matching techniques to identify suspicious patterns. The article describes the U.S. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Money Laundering Detection**, build a **economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary** for this defensive due diligence and uncertainty-preserving FININT topic. The artifact must note the typology descriptor, the bounded claim about **Money Laundering Detection**, the intent caveat, the uncertainty threshold, the no-accusation boundary, and the reviewer who owns escalation. Shape **Money Laundering Detection** work as a **location-and-entity evidence ledger** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Money Laundering Detection**: that a typology or pattern match is proof of intent rather than a flag requiring corroboration and alternative explanations.

Transfer task. Apply this module's safe boundary for **Money Laundering Detection** to another artifact while keeping defensive due diligence and uncertainty-preserving FININT and reviewer ownership explicit.

26.2.2.8 Lesson 8: FININT Supporting National Security: Pillars and Methods

Concept. FININT Supporting National Security: Pillars and Methods reads financial intelligence as due-diligence evidence that triggers review rather than proof of intent or guilt.

Why it matters. FININT Supporting National Security matters in the **Financial Intelligence and Economic-Security Due Diligence** lane because defensive due diligence and uncertainty-preserving FININT evidence must stay separate from judgment; evasion playbooks is a common failure.

Source support. FININT Supporting National Security: Pillars and Methods rests on [082, 2026]. Its anchor reference records: A 2025 article by Kevin Hk Chow in Modern Economy titled "Financial Intelligence: A Crucial Pillar of National Security." It argues that the module serves as a critical interface between economic systems and national security, used to detect and disrupt illicit financial networks tied to money laundering, terrorism financing, and transnational crime. Use it for the working definition that **FININT Supporting National Security: Pillars and Methods** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Network, 2026a]; [Network, 2026b].

Evidence to inspect. Ground **FININT Supporting National Security** in the evidence the row cites. [082, 2026] A 2025 article by Kevin Hk Chow in Modern Economy titled "Financial Intelligence: A Crucial Pillar of National Security." It argues that the module serves as a critical interface between economic systems and national security, used to detect and disrupt illicit financial networks tied to money laundering, terrorism financing, and transnational crime. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **FININT Supporting National Security**, build a **economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary** for this defensive due diligence and uncertainty-preserving FININT topic. The artifact must name the source descriptor, the bounded claim about **FININT Supporting National Security**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **FININT Supporting National Security** work as a **location-and-entity evidence ledger** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that FININT Supporting National Security: Pillars and Methods is optional whenever separate compliance-oriented risk analysis from evasion, attribution certainty, or targeting feels inconvenient.

Transfer task. Transfer **FININT Supporting National Security** to a second module by preserving defensive due diligence and uncertainty-preserving FININT, changing the source evidence, and naming a new reviewer.

26.2.3 Financial Intelligence (FININT) worked safe example: synthetic inputs, evidence, and review

Worked example: a sample nonprofit screens a synthetic supplier record for classroom due-diligence practice. [251, 2026]; [252, 2026].

Triangulation anchors. In module 17's worked-example section, directly verified anchors for the **Financial Intelligence and Economic-Security Due Diligence** lane include [Network, 2026a]; [Network, 2026b]; [of Foreign Assets Control, 2026]; [of Foreign Assets Control, 2019]. Use them to test

source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **geospatial and financial intelligence uncertainty**. Learners use a **location-and-entity evidence ledger** and keep this boundary visible: No facility targeting, pattern-of-life inference, evasion advice, or attribution certainty beyond evidence.

Frame. The classroom question centers on **FININT Foundations: Collection, Analysis, Reporting**. Excluded actions stay explicit, and the **Economic-Security Due-Diligence Lens** planning question is: Which financial, sanctions, export-control, or supplier-risk signal is being interpreted for lawful compliance or resilience?

Inputs. For the **FININT Foundations: Collection, Analysis, Reporting** scenario, use toy entity records, public sanctions-program descriptions, synthetic transaction summaries, and supplier-context notes. The Economic-Security Due-Diligence Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **FININT Foundations: Collection, Analysis, Reporting**, students check official list provenance, identify red flags, preserve beneficial-ownership uncertainty, and avoid evasion guidance. Pause whenever an inference about FININT Foundations: Collection, Analysis, Reporting appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **FININT Foundations: Collection, Analysis, Reporting** classroom scenario; unit artifact = location-and-entity evidence ledger; evidence = allowed inputs; method = defensive due diligence and uncertainty-preserving FININT; output = an economic-security packet with source links, uncertainty, red-flag rationale, and a compliance review owner; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **FININT Foundations: Collection, Analysis, Reporting** as "Economic-Security Due-Diligence Lens confirms it" is not enough. The revision ties the claim to defensive due diligence and uncertainty-preserving FININT, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **FININT Foundations: Collection, Analysis, Reporting** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

26.2.4 Financial Intelligence (FININT) practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Economic-Security Due-Diligence Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**.

Triangulation anchors. In module 17's practice-sequence section, directly verified anchors for the **Financial Intelligence and Economic-Security Due Diligence** lane include [Network, 2026a]; [Network, 2026b]; [of Foreign Assets Control, 2026]; [of Foreign Assets Control, 2019]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare FININT Foundations: Collection, Analysis, Reporting, Financial due-diligence typology exercise using synthetic records and compliance boundaries, Non-state actor indicator review with attribution caution and governance boundaries; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Financial Intelligence and Economic-Security Due Diligence** lane.
2. Frame	Answer the lens question: Which financial, sanctions, export-control, or supplier-risk signal is being interpreted for lawful compliance or resilience?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for FININT Foundations: Collection, Analysis, Reporting: economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the location-and-entity evidence ledger fields for FININT Foundations: Collection, Analysis, Reporting.	Unit profile note.	Evidence artifacts include geospatial quality note, temporal caveat.
4. Challenge	Test the misconception that FININT Foundations: Collection, Analysis, Reporting establishes intent without reviewing alternative explanations.	Failure-mode note.	The artifact applies the key distinction: separate compliance-oriented risk analysis from evasion, attribution certainty, or targeting.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

26.2.4.1 Financial Intelligence (FININT) instructor notes: source reasoning, review points, and studio focus

Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**. [251, 2026]; [252, 2026].

26.2.4.2 Financial Intelligence (FININT) extension exercise: peer validation and refresh trigger review

Evidence anchor. Section 26; [251, 2026].

Have learners swap artifacts and apply the **Economic-Security Due-Diligence Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**.

26.2.5 Financial Intelligence (FININT) knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 26; [251, 2026].

1. Explain how **FININT Foundations: Collection, Analysis, Reporting** is defined here; name the source descriptor that supports the definition.
2. Contrast **FININT Foundations: Collection, Analysis, Reporting** with **Financial due-diligence typology exercise using synthetic records and compliance boundaries** using the **Economic-Security Due-Diligence Lens** artifact fields.
3. Identify one failure mode from the **Financial Intelligence and Economic-Security Due Diligence** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which red flag requires escalation, and what evidence is still missing?
5. Correct this misconception: that FININT Foundations: Collection, Analysis, Reporting establishes intent without reviewing alternative explanations.

26.2.5.1 Financial Intelligence (FININT) answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **FININT Foundations: Collection, Analysis, Reporting** without source evidence, uncertainty, or a safe transfer task.

26.3 Financial Intelligence (FININT) assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 26; [251, 2026].

26.3.1 Financial Intelligence (FININT) evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 26; [251, 2026].

26.3.2 Financial Intelligence (FININT) transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 26; [251, 2026].

26.3.2.1 Financial Intelligence (FININT) lineage and source tradition: profile, concepts, and first anchors This sits in the **Financial Intelligence and Economic-Security Due Diligence** lineage: defensive economic intelligence that links financial-crime signals, sanctions programs, export controls, beneficial-ownership uncertainty, and supply-chain due diligence to lawful compliance and policy analysis. [251, 2026]; [252, 2026].

26.3.2.2 Financial Intelligence (FININT) working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 26; [251, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**, with provenance and reviewability throughout.

26.3.2.3 Financial Intelligence (FININT) knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [251, 2026]; [252, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

26.3.2.4 Financial Intelligence (FININT) transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 26; [251, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**.
- **Evidence contract:** keep the **Financial Intelligence and Economic-Security Due Diligence** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

26.3.2.5 Financial Intelligence (FININT) profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 26; [251, 2026].

The matched profile emphasizes defensive economic intelligence that links financial-crime signals, sanctions programs, export controls, beneficial-ownership uncertainty, and supply-chain due diligence to lawful compliance and policy analysis. The method stack is typology-to-control mapping, sanctions-program review, beneficial ownership uncertainty notes, export-control red-flag triage, supplier risk registers, and compliance-oriented analytic memos; the local topic cluster is **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**.

26.3.3 Financial Intelligence (FININT) evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 26; [251, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Financial Intelligence and Economic-Security Due Diligence** profile tells reviewers what evidence is strong enough for the module artifact built around **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**.

26.3.3.1 Financial Intelligence (FININT) guide source spine: inherited keys and local citation roles Primary guide citations: [251, 2026]; [252, 2026]; [254, 2026]; [273, 2026]; [274, 2026]; [275, 2026]; [286, 2026]; [287, 2026]; [292, 2026]; [079, 2026]; [080, 2026]; [081, 2026]; [082, 2026]; [302, 2026]; [297, 2026].

26.3.3.2 Financial Intelligence (FININT) verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [251, 2026]; [252, 2026].

Tier	What counts	How it is used
Source guide	[251, 2026]; [252, 2026]; [254, 2026]; [273, 2026]; [274, 2026]; [275, 2026]; [286, 2026]; [287, 2026]; [292, 2026]; [079, 2026]; [080, 2026]; [081, 2026]; [082, 2026]; [302, 2026]; [297, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 17's source-canon section, directly verified anchors for the **Financial Intelligence and Economic-Security Due Diligence** lane include [Network, 2026a]; [Network, 2026b]; [of Foreign Assets Control, 2026]; [of Foreign Assets Control, 2019]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries** and [251, 2026]; [252, 2026], but only directly verified source URLs are encoded as citations.

26.3.3.3 Financial Intelligence (FININT) intelligence practice lens: evidence artifact and safety check Practice lens: **Economic-Security Due-Diligence Lens** for **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**. [251, 2026]; [252, 2026].

Planning question: Which financial, sanctions, export-control, or supplier-risk signal is being interpreted for lawful compliance or resilience?

Evidence artifact: economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary.

Validation rule: verify official list source, typology provenance, beneficial-ownership uncertainty, export-control relevance, and non-evasion framing. Applied to **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**.

Handoff contract: handoff separates raw source, entity hypothesis, compliance control, analytic judgment, and recommended defensive next review.

Safety check: exclude sanctions evasion, laundering methods, threshold gaming, procurement bypasses, and tailored targeting of real firms.

26.3.3.4 Financial Intelligence (FININT) runtime-to-reader map: generated sections and verifier surfaces **Evidence anchor.** Section 26; [251, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	17.99	17.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Financial Intelligence (FININT) to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Bounded autonomy, procurement, incident-response, and assurance studio	17.101	17.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Financial Intelligence (FININT)	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Model-card, recoverability, retention, and learner-support evidence package	17.102	17.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Financial Intelligence (FININT)	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
FININT Foundations: Collection, Analysis, Reporting	17.1	17.1 FININT Foundations: Collection, Analysis, Reporting	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Financial due-diligence typology exercise using synthetic records and compliance boundaries	17.2	17.2 source title transformed into safe curriculum treatment; original: Suspicious Activity Reports (SARs) and Financial Intelligence Units	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Non-state actor indicator review with attribution caution and governance boundaries	17.3	17.3 source title transformed into safe curriculum treatment; original: Terrorist Financing: Identification, Typologies, Interdiction	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
The SWIFT System and Intelligence Collection	17.4	17.4 The SWIFT System and Intelligence Collection	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Cryptocurrency as Covert Finance: Monero, Mixers, Bridges	17.5	17.5 Cryptocurrency as Covert Finance: Monero, Mixers, Bridges	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Economic Warfare and FININT as a Strategic Tool	17.6	17.6 Economic Warfare and FININT as a Strategic Tool	Economic-Security Due-Diligence Lens	economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary	exclude sanctions evasion, laundering methods, threshold gaming, procurement bypasses, and tailored targeting of real firms
Financial due-diligence typology exercise using synthetic records and compliance boundaries	17.7	17.7 source title transformed into safe curriculum treatment; original: Money Laundering Detection: Data Mining and Matching Techniques	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
FININT Supporting National Security: Pillars and Methods	17.8	17.8 FININT Supporting National Security: Pillars and Methods	Economic-Security Due-Diligence Lens	economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary	exclude sanctions evasion, laundering methods, threshold gaming, procurement bypasses, and tailored targeting of real firms

26.3.3.5 Financial Intelligence (FININT) reusable subsection contract: topic rows, artifacts, and safety duties **Evidence anchor.** Section 26; [251, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
FININT Foundations: Collection, Analysis, Reporting	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Financial due-diligence typology exercise using synthetic records and compliance boundaries	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Non-state actor indicator review with attribution caution and governance boundaries	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
The SWIFT System and Intelligence Collection	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Cryptocurrency as Covert Finance: Monero, Mixers, Bridges	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Economic Warfare and FININT as a Strategic Tool	Economic-Security Due-Diligence Lens	economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary	exclude sanctions evasion, laundering methods, threshold gaming, procurement bypasses, and tailored targeting of real firms

Lesson topic	Practice lens	Evidence artifact	Safety check
Money Laundering Detection: Financial due-diligence typology exercise using synthetic records and compliance boundaries	Economic-Security Due-Diligence Lens	economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary	exclude sanctions evasion, laundering methods, threshold gaming, procurement bypasses, and tailored targeting of real firms
FININT Supporting National Security: Pillars and Methods	Economic-Security Due-Diligence Lens	economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary	exclude sanctions evasion, laundering methods, threshold gaming, procurement bypasses, and tailored targeting of real firms

26.3.3.6 Financial Intelligence (FININT) annotated source ledger: real titles and local contribution Each source cited by this **Financial Intelligence and Economic-Security Due Diligence** module is paired below with its real title and a one-line note on what it contributes to **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**.

Source	Cited work	What it contributes	Status
[251, 2026]	European Data Governance Act	The European Commission page explaining the Data Governance Act, an EU regulation that became applicable in September 2023 to build trust in data sharing and ease reuse of data. It outlines four mechanisms: facilitating reuse of protected public-sector data, establishing trusted data intermediaries, enabling voluntary data sharing by citizens and businesses, and removing barriers to cross-sector and cross-border data use.	verified source-guide
[252, 2026]	Data Act Explained	An official European Commission explainer on the EU Data Act, which became applicable on 12 September 2025.	verified source-guide
[254, 2026]	A European Strategy for Data	An official European Commission page outlining the European Strategy for Data, which aims to create a single market for data to support competitiveness and data sovereignty. It describes initiatives such as Common European Data Spaces, opening high-value public datasets, and investment in cloud and data-processing capacity, supported by the Data Governance Act and the Data Act. The page frames data sharing as a driver of innovation balanced with privacy and European values.	verified source-guide
[273, 2026]	WCAG 2 Overview	The W3C Web Accessibility Initiative overview of the Web Content Accessibility Guidelines (WCAG), an international standard for making web content accessible to people with disabilities. It explains that WCAG is organized around four principles (perceivable, operable, understandable, robust) with testable success criteria at three conformance levels (A, AA, AAA), and covers versions 2.0, 2.1, and 2.2.	verified source-guide
[274, 2026]	CAST Universal Design for Learning Guidelines version 3.0	The official CAST website for the Universal Design for Learning (UDL) Guidelines version 3.0, released in 2024. The framework offers research-based guidance for designing inclusive learning environments and is organized around three principles: Engagement (motivation and emotional support), Representation (accessible presentation of information), and Action and Expression (diverse means of participation and communication).	verified source-guide

Source	Cited work	What it contributes	Status
[275, 2026]	Fact Sheet: New Rule on the Accessibility of Web Content and Mobile Apps Provided by State and Local Governments	A US Department of Justice fact sheet explaining the 2024 ADA Title II rule requiring state and local governments to make their web content and mobile apps accessible. It establishes WCAG 2.1 Level AA as the technical standard, applies to entities such as schools, courts, libraries, and transit agencies, and sets compliance deadlines of April 2027 for larger jurisdictions and April 2028 for smaller ones.	verified source-guide
[286, 2026]	Model Cards for Model Reporting	The arXiv abstract for "Model Cards for Model Reporting" (2018) by Mitchell, Wu, Zaldivar, and colleagues, which introduces a framework for transparent documentation of machine learning models. Model cards are short accompanying documents that report a model's benchmarked performance across varied conditions, including different cultural, demographic, and phenotypic groups, along with intended use, evaluation methodology, and deployment considerations.	verified source-guide
[287, 2026]	Datasheets for Datasets	A 2018 arXiv paper proposing 'datasheets for datasets,' a standardized documentation framework for machine learning datasets modeled on electronic component datasheets. The authors argue the field lacks consistent dataset documentation, which creates risk in high-stakes applications, and propose that datasets be accompanied by documentation covering motivation, composition, collection process, recommended uses, and test results.	verified source-guide
[292, 2026]	Assessing Risks and Impacts of AI (ARIA): Pilot Evaluation Report	The ARIA 0.1 pilot evaluation report documents NIST's methodology for systematically assessing AI applications for risks and societal impacts, using a multi-layered evaluation approach across five participating organizations and seven submitted AI applications. The pilot employed three evaluation scenarios and three testing levels: model testing, red teaming, and field testing, supplemented by dialogue annotation, tester questionnaires, and structured measurement trees.	verified source-guide
[079, 2026]	Financial intelligence	The Wikipedia article on financial intelligence (FININT), defined as gathering information about the financial affairs of entities of interest to understand their nature, capabilities, and intentions. It outlines two core components: collection, in which Financial Intelligence Units gather transaction data and suspicious activity reports from banks, and analysis, in which specialists use data mining to detect tax evasion, money laundering, and terrorist financing.	verified source-guide context; do not use as primary analytic support

Source	Cited work	What it contributes	Status
[080, 2026]	Financial intelligence	A Wikipedia article on financial intelligence (FININT), the gathering and analysis of information about financial transactions to detect illicit activity such as money laundering, tax evasion, and terrorist financing. It distinguishes two core functions: collection of raw transaction data and suspicious activity reports by government financial intelligence units, and analysis using data-matching techniques to identify suspicious patterns. The article describes the U.S.	verified source-guide context; do not use as primary analytic support
[081, 2026]	Financial intelligence	The Citizendium 'Financial intelligence' article was never written; the page is empty. Use an authoritative alternative source for financial intelligence definitions.	verified source-guide
[082, 2026]	Financial Intelligence: A Crucial Pillar of National Security	A 2025 article by Kevin Hk Chow in Modern Economy titled "Financial Intelligence: A Crucial Pillar of National Security." It argues that Financial Intelligence (FININT) serves as a critical interface between economic systems and national security, used to detect and disrupt illicit financial networks tied to money laundering, terrorism financing, and transnational crime.	verified source-guide
[302, 2026]	National Geospatial-Intelligence Agency About Us	The official "About Us" page of the National Geospatial-Intelligence Agency (NGA), a U.S. Department of Defense and intelligence community organization. It describes NGA's mission of delivering geospatial intelligence, or GEOINT, to support military operations, policymakers, and first responders, spanning imagery analysis, mapping, geodesy, and navigation safety.	verified source-guide
[297, 2026]	Intelligence Community Directive 203: Analytic Standards	Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products.	original source-guide

Where this sits. This module's overview is Section 26; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

26.3.4 Financial Intelligence (FININT) governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 26; [251, 2026].

26.3.5 Financial Intelligence (FININT) analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 17's governance-boundary section, directly verified anchors for the **Financial Intelligence and Economic-Security Due Diligence** lane include [Network, 2026a]; [Network, 2026b]; [of Foreign Assets Control, 2026]; [of Foreign Assets Control, 2019]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Research lane: **Financial Intelligence and Economic-Security Due Diligence** for **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**. [251, 2026]; [252, 2026].
Curriculum topic spine: FININT Foundations: Collection, Analysis, Reporting, **Financial due-diligence typology exercise using synthetic records and compliance boundaries**, **Non-state actor indicator review with attribution caution and governance boundaries**.
Verified anchor cluster: [Network, 2026a]; [Network, 2026b]; [of Foreign Assets Control, 2026]; [of Foreign Assets Control, 2019]; [Force, 2025]; [Force, 2021]; [for International Settlements, 2021].
Conceptual depth: defensive economic intelligence that links financial-crime signals, sanctions programs, export controls, beneficial-ownership uncertainty, and supply-chain due diligence to lawful compliance and policy analysis.
Method stack: typology-to-control mapping, sanctions-program review, beneficial ownership uncertainty notes, export-control red-flag triage, supplier risk registers, and compliance-oriented analytic memos.
Composability contract: entities, transactions, sanctions programs, red flags, supplier evidence, legal constraints, and analytic judgments remain separately reviewable.
Known failure modes: evasion playbooks, threshold gaming, overconfident attribution, stale sanctions data, unverified beneficial ownership, and confusing compliance screening with intelligence certainty.
Defensive boundary: FININT and economic-security examples remain compliance, policy, and resilience oriented; they do not explain how to launder funds, evade sanctions, bypass export controls, or target real firms. Applied to **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**.

Anchor	Why it matters here
[Network, 2026a]	Official FININT source for AML/CFT advisories, typology awareness, sanctions-evasion warnings, red flags, and compliance-oriented monitoring. Checked as of 2026-05-21; role: curriculum_anchor.
[Network, 2026b]	Official FinCEN source for beneficial-ownership reporting, entity transparency, exemptions, and compliance-oriented analysis. Checked as of 2026-05-21; role: curriculum_anchor.
[of Foreign Assets Control, 2026]	Official OFAC sanctions-program library for understanding legal program structure, list maintenance, and compliance-oriented economic statecraft. Checked as of 2026-05-21; role: curriculum_anchor.
[of Foreign Assets Control, 2019]	Official OFAC compliance framework for management commitment, risk assessment, internal controls, testing, auditing, and training. Checked as of 2026-05-21; role: curriculum_anchor.
[Force, 2025]	Official international AML/CFT/CPF standard for risk-based controls, beneficial ownership, information sharing, supervision, and mutual evaluation. Checked as of 2026-05-21; role: curriculum_anchor.
[Force, 2021]	Official FATF guidance for virtual-asset risk, VASP supervision, travel-rule compliance, and non-evasion FININT education. Checked as of 2026-05-21; role: curriculum_anchor.
[for International Settlements, 2021]	Official BIS policy source for financial technology, market structure, data, network effects, regulation, privacy, and stability tradeoffs. Checked as of 2026-05-21; role: curriculum_anchor.

26.3.5.1 Financial Intelligence (FININT) evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **Financial Intelligence and Economic-Security Due Diligence** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [251, 2026]; [252, 2026].

26.3.6 Financial Intelligence (FININT) agentic boundary: assist, approve, block, and record

Evidence anchor. Section 26; [251, 2026].
AGEINT translation is bounded by the **Financial Intelligence and Economic-Security Due Diligence** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**.

26.3.6.1 Financial Intelligence (FININT) permitted defensive utility: curriculum uses and safe outputs

Evidence anchor. Section 26; [251, 2026].
The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**.

26.3.6.2 Financial Intelligence (FININT) excluded operational boundary: blocked actions and stop rules

Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [251, 2026]; [252, 2026] and **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

26.3.7 Financial Intelligence (FININT) governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 26; [251, 2026].
Governance is practiced as a gate on the **Financial Intelligence and Economic-Security Due Diligence** lane. Learners use the **Economic-Security Due-Diligence Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and

when an agent-assisted artifact must stop for human review while using **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**.

26.3.7.1 Financial Intelligence (FININT) governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [251, 2026]; [252, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Financial Intelligence and Economic-Security Due Diligence** failure modes and the **Economic-Security Due-Diligence Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

26.3.7.2 Financial Intelligence (FININT) evidence package handoff: appendices, records, and reuse **Evidence anchor.** Section 26; [251, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Economic-Security Due-Diligence Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**.

26.3.7.3 Financial Intelligence (FININT) current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**. [251, 2026]; [252, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_fincen_advisories` for **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**?	FinCEN Alerts, Advisories, Notices, Bulletins, and Fact Sheets; lane `financial_economic_security`; checked 2026-05-21.	economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary; Official FININT source for AML/CFT advisories, typology awareness, sanctions-evasion warnings, red flags, and compliance-oriented monitoring.
What does the module inherit from `official_fincen_boi` for **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**?	Beneficial Ownership Information Reporting; lane `financial_economic_security`; checked 2026-05-21.	economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary; Official FinCEN source for beneficial-ownership reporting, entity transparency, exemptions, and compliance-oriented analysis.
What does the module inherit from `official_ofac_sanctions_programs` for **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**?	Sanctions Programs and Country Information; lane `financial_economic_security`; checked 2026-05-21.	economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary; Official OFAC sanctions-program library for understanding legal program structure, list maintenance, and compliance-oriented economic statecraft.
What does the module inherit from `official_ofac_compliance_commitments` for **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**?	A Framework for OFAC Compliance Commitments; lane `financial_economic_security`; checked 2026-05-21.	economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary; Official OFAC compliance framework for management commitment, risk assessment, internal controls, testing, auditing, and training.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 26; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

26.3.8 Financial Intelligence (FININT) assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 26; [251, 2026].

26.3.9 Financial Intelligence (FININT) assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 26; [251, 2026].

26.3.9.1 Financial Intelligence (FININT) capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries** and [251, 2026]; [252, 2026].

26.3.9.2 Financial Intelligence (FININT) instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries** and [251, 2026]; [252, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

26.3.9.3 Financial Intelligence (FININT) assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
FININT Foundations: Collection, Analysis, Reporting	Completed **economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Financial due-diligence typology exercise using synthetic records and compliance boundaries	Completed **economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Non-state actor indicator review with attribution caution and governance boundaries	Completed **economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

26.3.10 Financial Intelligence (FININT) refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [251, 2026]; [252, 2026] and **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**.

26.3.10.1 Financial Intelligence (FININT) refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**. The local signals begin with [251, 2026]; [252, 2026].

26.3.10.2 Financial Intelligence (FININT) claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**, and the source spine for these checks begins with [251, 2026]; [252, 2026].

26.3.11 Financial Intelligence (FININT) reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [251, 2026]; [252, 2026].

Triangulation anchors. In module 17's review-checklist section, directly verified anchors for the **Financial Intelligence and Economic-Security Due Diligence** lane include [Network, 2026a]; [Network, 2026b]; [of Foreign Assets Control, 2026]; [of Foreign Assets Control, 2019]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries**. [251, 2026]; [252, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.

- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

26.3.12 Financial Intelligence (FININT) learning-path links: module map, overview, and curriculum atlas

These links keep **FININT Foundations: Collection, Analysis, Reporting; Financial due-diligence typology exercise using synthetic records and compliance boundaries** paired with the orientation atlas, the parent unit, and the previous and next modules, so a reader can trace which claims and caveats are inherited rather than re-derived here. Anchored at [251, 2026]; [252, 2026].
Section 2, Section 24, Section 25, Section 27

27 PSYCHOLOGICAL OPERATIONS AND INFLUENCE

27.1 PSYCHOLOGICAL OPERATIONS AND INFLUENCE learning spine and source route: unit purpose, module order, and evidence handoff

Evidence anchor. Section 27; [238, 2026].

27.1.1 information-integrity and influence analysis discipline spine: domain question and learning focus

Evidence anchor. Section 27; [238, 2026].
This unit teaches **information-integrity and influence analysis**. Influence lessons analyze narratives, provenance, audience harm, attribution caution, and transparent resilience education without persuasion design.

27.1.2 information-integrity and influence analysis source-use contract: citation roles and evidence limits

Evidence anchor. Section 27; [238, 2026].
Use CISA and NATO anchors for foreign influence, information threats, public resilience, and transparent mitigation claims.

27.1.3 information-integrity and influence analysis practice artifact: recurring packet and retained evidence

Evidence anchor. Section 27; [238, 2026].
The recurring practice artifact is a **narrative-risk and resilience map** that draws on narrative provenance chain, audience-harm note, attribution caveat, and transparent response option. The unit keeps its learning spine explicit. Learners separate message observation from attribution, identify harm, and choose transparent education or correction options.

27.1.4 information-integrity and influence analysis safety boundary: accountable, synthetic, and evidence-bounded limits

No covert persuasion, microtargeting, manipulation, or campaign design.
This unit introduces the part's governing question, evidence artifacts, source-support spine, and capstone thread before the individual modules begin. [238, 2026]; [239, 2026].
Learners carry one unit capstone thread through the part: define an accountable intelligence question, bind it to source-quality constraints, produce a reviewable artifact, test the artifact against failure modes, and hand it off with enough context for another analyst or instructor to audit. The capstone remains public, synthetic, or owned-lab throughout; its first source anchors are [238, 2026]; [239, 2026].
This unit's deliverables are a source-canon card, claim/evidence ledger, safe-practice lab packet, failure-mode note, instructor rubric, and debrief memo. The full source-lane and evidence-package ledgers appear in the orientation and appendices; this unit introduction keeps only the learner-facing spine for [238, 2026]; [239, 2026].
This unit's safety gates are scope authorization, rights review, data provenance, tool allowlisting, human oversight, rollback, and evidence-bounded output. A missing gate turns the activity into a tabletop, audit, or written governance exercise until the gate is restored against [238, 2026]; [239, 2026].
Capstone thread:

Phase	Artifact	Review gate
Question	accountable learning question and excluded-action list	instructor confirms scope, allowed data, and rights impact
Source canon	source-lane map with guide citations, verified anchors, and refresh dates	citation keys resolve and source identity lock remains stable
Evidence ledger	claim, evidence, uncertainty, confidence, and reviewer register	every material claim has a source, caveat, and owner
Safe lab	synthetic or public dataset packet, tool allowlist, and stop conditions	no live target, private data, external action, or unsafe cyber-physical step
Assurance	evaluation rubric, failure-mode drill, rights map, and remediation note	human reviewer signs off before presentation or reuse
Debrief	capstone memo with lessons, residual risk, refresh triggers, and handoff owner	all unresolved questions and future approvals are explicit

Research lane: Cognitive Security and Influence Resilience. Core anchors: [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]. Conceptual focus: protecting attention, belief formation, and decision quality without turning resilience education into manipulation. Composability contract: separate descriptive analysis, normative assessment, response options, and protected-audience considerations. **Practice lens:** Cognitive-Resilience Lens; How does the module protect autonomy, attention, trust, and decision quality without designing persuasion? [238, 2026]; [239, 2026].

27.1.5 PSYCHOLOGICAL OPERATIONS AND INFLUENCE visual navigation and module map: evidence flow, order, and safety cues

The unit uses Figure 64 and Figure 65 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 26, Section 28.

27.1.6 PSYCHOLOGICAL OPERATIONS AND INFLUENCE module roster and source-lane inventory: citations, lanes, and learner route

Module	Section reference	Source spine
PSYOP and MISO Doctrine	Section 28	[238, 2026]; [239, 2026]; [242, 2026]; [276, 2026]; [277, 2026]; [284, 2026]; [288, 2026]; [289, 2026]; [293, 2026]; [083, 2026]; [084, 2026]; [085, 2026]; [086, 2026]; [087, 2026]; [302, 2026]; [297, 2026]; [308, 2026]; [311, 2026].
Active Measures and Disinformation	Section 29	[238, 2026]; [239, 2026]; [240, 2026]; [278, 2026]; [279, 2026]; [283, 2026]; [290, 2026]; [291, 2026]; [294, 2026]; [088, 2026]; [089, 2026]; [090, 2026]; [091, 2026]; [092, 2026]; [093, 2026]; [094, 2026]; [095, 2026]; [096, 2026]; [308, 2026]; [311, 2026].

Module	Section reference	Source spine
Social Engineering	Section 30	[238, 2026]; [240, 2026]; [242, 2026]; [280, 2026]; [281, 2026]; [282, 2026]; [292, 2026]; [295, 2026]; [296, 2026]; [097, 2026]; [098, 2026]; [099, 2026]; [100, 2026]; [300, 2026]; [304, 2026]; [306, 2026]; [308, 2026]; [311, 2026].
Information Warfare and Cognitive Security	Section 31	[238, 2026]; [239, 2026]; [244, 2026]; [273, 2026]; [276, 2026]; [285, 2026]; [286, 2026]; [290, 2026]; [294, 2026]; [101, 2026]; [102, 2026]; [103, 2026]; [104, 2026]; [105, 2026]; [095, 2026]; [096, 2026]; [106, 2026]; [003, 2026]; [107, 2026].

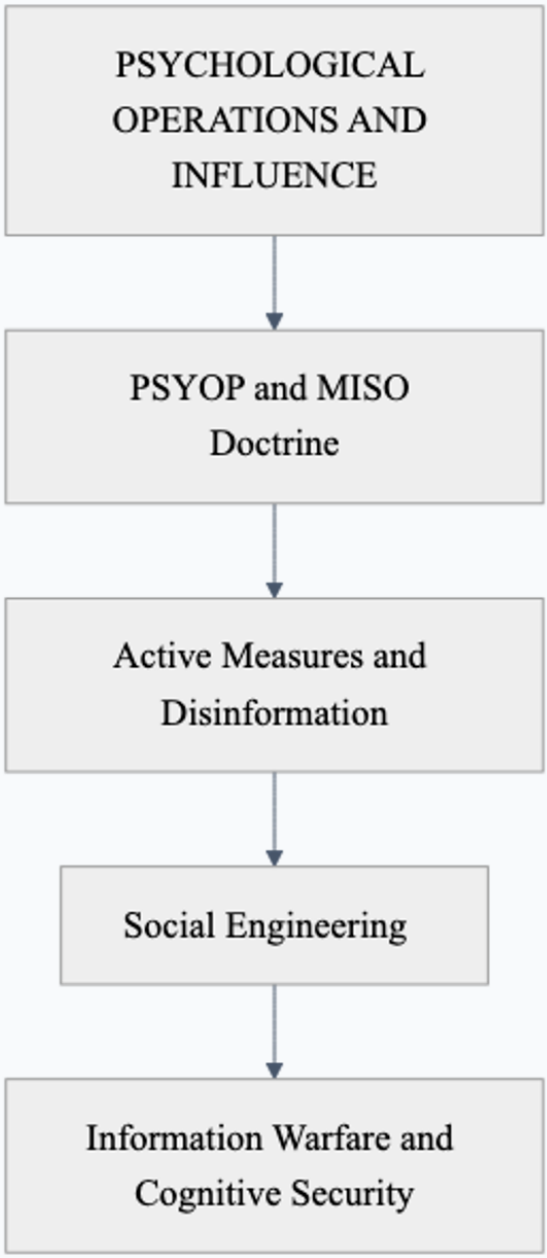


Figure 64: The unit module map traces the part's chapters as a linear reading sequence. Its reader value is to make 4 module nodes in the unit's ordered, source-backed reading sequence from its first module to its last visible at a glance, with the psychological operations and influence section as the source section and defensive review as the boundary.

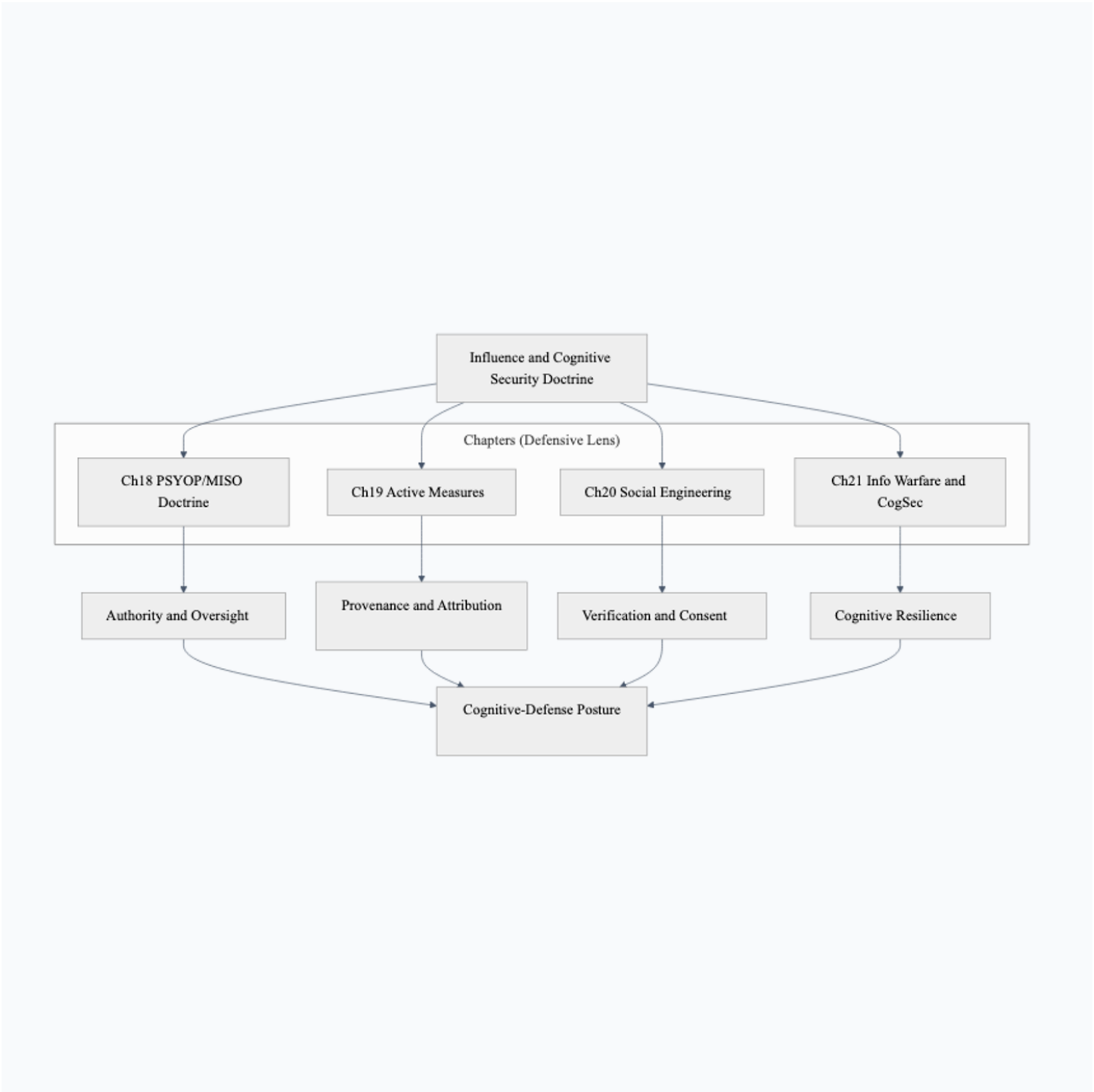


Figure 65: Studied defensively, this Part is a doctrine-and-countermeasure spine: each influence chapter is matched to the detection signals and cognitive-resilience controls that defend against it. In the psychological operations and influence section, it lets readers compare Influence and Cognitive Security Doctrine, Chapters (Defensive Lens), Ch18 PSYOP/MISO Doctrine, and Ch19 Active Measures so the visual functions as a traceable course aid rather than an unscoped assertion.

28 PSYOP and MISO Doctrine

28.0.1 PSYOP and MISO Doctrine figures and course links: visual evidence, source flow, and navigation

The module uses Figure 66 and Figure 64 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 27, Section 29.
This module teaches the **Cognitive Security and Influence Resilience** lane through a bounded, source-backed coursebook chapter. [238, 2026]; [239, 2026].

28.1 Cognitive Security and Influence Resilience frame for PSYOP and MISO Doctrine: source context, topic focus, and reader task

Evidence anchor. Section 28; [238, 2026].

28.1.1 PSYOP and MISO Doctrine orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 28; [238, 2026].

28.1.2 PSYOP and MISO Doctrine conceptual primer: source context, core model, and reader task

This chapter teaches cognitive security as protection of attention, trust, memory, and decision quality without creating manipulation. The chapter uses **Cognitive-Resilience Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2**.
The central distinction is to separate analysis of influence from persuasion design. Core topics include **Cognitive influence-analysis case review using sample materials; Military Information Support Operations (MISO): JP 3-13.2; Tactical PSYOP TTP: Cognitive influence-analysis case review using sample materials**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [238, 2026]; [239, 2026].
Learners move from vocabulary and the **Cognitive-Resilience Lens** distinction through topic lessons on **Cognitive influence-analysis case review using sample materials** with evidence and misconception checks, then assemble a **narrative-risk map with provenance, uncertainty, audience harms, and response options** with safety and rights gates.

28.1.3 PSYOP and MISO Doctrine learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 28; [238, 2026].

- Connect **Cognitive influence-analysis case review using sample materials and Military Information Support Operations (MISO): JP 3-13.2** to **Cognitive Security and Influence Resilience** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate analysis of influence from persuasion design; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as counter-messaging as manipulation, overclaiming intent, pathologizing audiences, and collapsing uncertainty into moral certainty, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: practice uses benign simulations and resilience education; it does not create persuasion campaigns, impersonation, or deception plans.

28.1.4 PSYOP and MISO Doctrine core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 28; [238, 2026].

Term	Working definition
Narrative provenance	where a claim, frame, or story came from and how it spread
Prebunking	transparent education that helps people recognize misleading patterns before exposure
Audience harm	a privacy, dignity, autonomy, or trust risk for people receiving information
Attribution caution	the rule that intent and origin claims need strong evidence
Resilience response	a transparent education, correction, or process improvement that avoids manipulation
MISO boundary	the line between accountable public messaging analysis and covert influence design
Inoculation	building recognition of manipulation tactics without deploying persuasion against a population
Cognitive influence-analysis case review using…	Key terms: Cognitive, influence, analysis.
Military Information Support Operations (MISO):…	Key terms: Military, Information, Support.

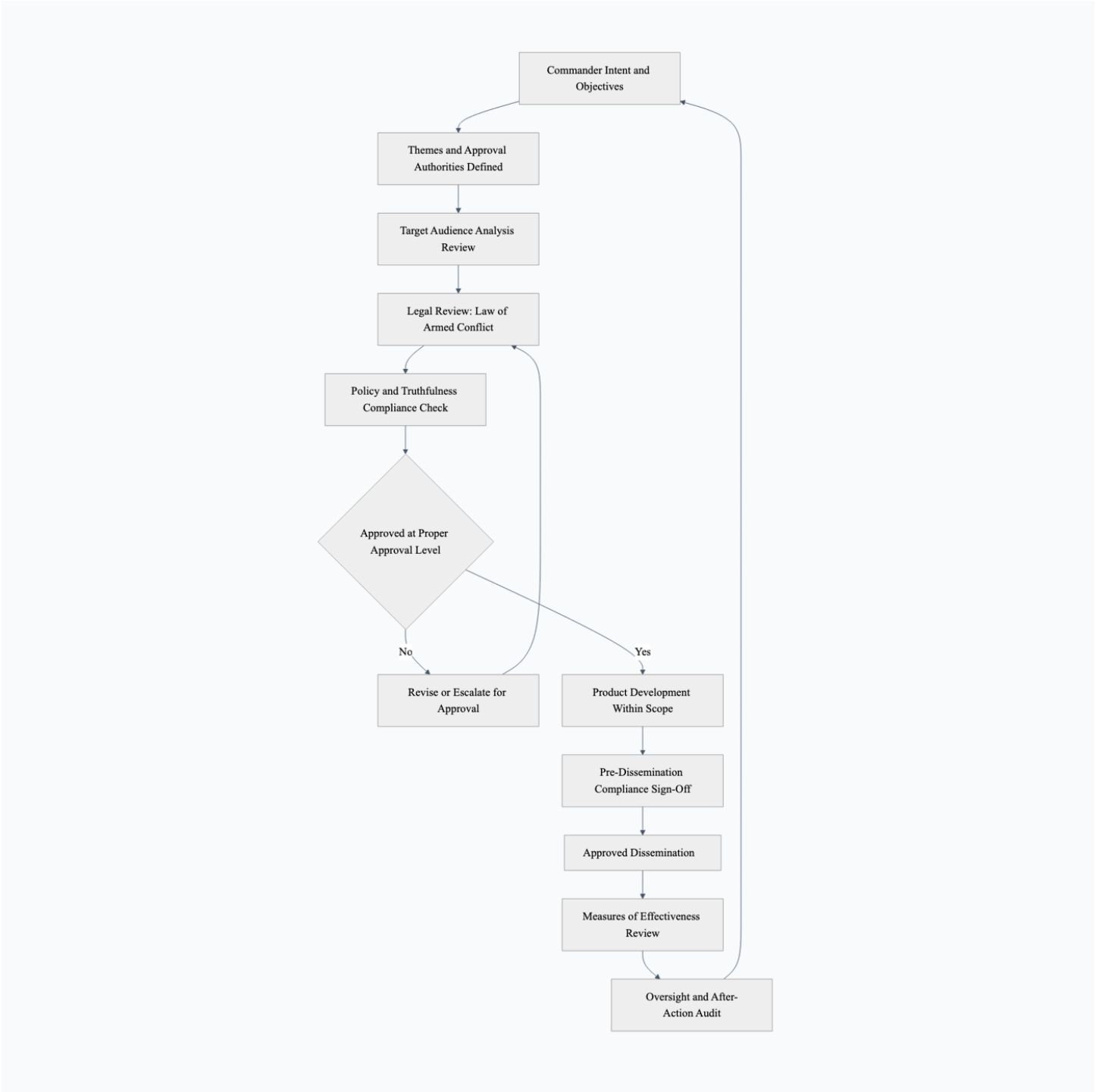


Figure 66: A doctrinal governance view showing how influence products must pass through legal, policy, and approval-authority gates before approved dissemination and after-action audit. The captioned view belongs to the psychological operations and influence / psyop and miso doctrine section and should be read as a map of Commander Intent and Objectives, Themes and Approval Authorities Defined, Target Audience Analysis Review, and Legal Review: Law of Armed Conflict, not as a capability score or live-task instruction.

28.2 Cognitive-Resilience Lens path for PSYOP and MISO Doctrine: lesson cluster, safe artifact, and review

Evidence anchor. Section 28; [238, 2026].

28.2.1 PSYOP and MISO Doctrine practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 28; [238, 2026].

28.2.2 PSYOP and MISO Doctrine topic lessons: source-backed concepts and transfer tasks

This module builds cognitive security as protection of attention, trust, memory, and decision quality without creating manipulation. The sequence opens with **Cognitive influence-analysis case review using sample materials**, **Military Information Support Operations (MISO): JP 3-13.2**, **Tactical PSYOP TTP: Cognitive influence-analysis case review using sample materials** and applies the **Cognitive-Resilience Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 64; module overview Section 28; curriculum atlas Section 2.

Triangulation anchors. In module 18's topic-lessons section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

28.2.2.1 Lesson 1: Cognitive influence-analysis case review using sample materials

Concept. Cognitive influence-analysis case review using sample materials studies influence doctrine as audience analysis, message integrity, and ethics—not as manipulation technique.

Why it matters. Cognitive influence-analysis case review matters in the **Cognitive Security and Influence Resilience** lane because information-integrity analysis and resilience education evidence must stay separate from judgment; treating resilience labels as permission to skip provenance review is a common failure.

Source support. Cognitive influence-analysis case review using sample materials rests on [083, 2026] and [084, 2026]. The closest source to this row notes: It establishes organizational structure, command relationships, planning processes, and approval authorities for integrating psychological operations into joint military campaigns and peacetime activities. Use them for the claim that **Cognitive influence-analysis case review using sample materials** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Cognitive influence-analysis case review**, work from the cited evidence behind this row. [083, 2026] Joint Publication 3-53, the US Department of Defense joint doctrine for psychological operations. It establishes organizational structure, command relationships, planning processes, and approval authorities for integrating psychological operations into joint military campaigns and peacetime activities. [084, 2026] Joint Publication 3-53, Doctrine for Joint Psychological Operations (Joint Chiefs of Staff, 10 July 1996). This US military doctrine document establishes the doctrinal basis for planning and conducting psychological operations in support of joint military operations. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Cognitive influence-analysis case review**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Cognitive influence-analysis case review using**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Cognitive influence-analysis case review** work as a **narrative-risk and resilience map** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Cognitive influence-analysis case review**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **Cognitive influence-analysis case review** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

28.2.2.2 Lesson 2: Military Information Support Operations (MISO): JP 3-13.2

Concept. Military Information Support Operations (MISO): JP 3-13.2 studies influence doctrine as audience analysis, message integrity, and ethics—not as manipulation technique.

Why it matters. Analysts use **Military Information Support Operations (MISO)** to separate analysis of influence from persuasion design. A defensible treatment names the judgment it enables for information-integrity analysis and resilience education review, the proof limit that counter-messaging as manipulation would otherwise hide, and the reviewer accountable for challenge.

Source support. Military Information Support Operations (MISO): JP 3-13.2 rests on [085, 2026]. Its anchor reference records: It sets forth joint doctrine to govern the activities and performance of the Armed Forces. Use it for pinning down the scope of **Military Information Support Operations (MISO): JP 3-13.2**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Military Information Support Operations (MISO)**, reason from the sources cited in this row. [085, 2026] It sets forth joint doctrine to govern the activities and performance of the Armed Forces. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Military Information Support Operations (MISO)**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must name the source descriptor, the bounded claim about **Military Information Support Operations**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Military Information Support Operations (MISO)** work as a **narrative-risk and resilience map** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that Military Information Support Operations (MISO): JP 3-13.2 can be used while ignoring the rule to separate analysis of influence from persuasion design.

Transfer task. Transfer **Military Information Support Operations (MISO)** to a second module by preserving information-integrity analysis and resilience education, changing the source evidence, and naming a new reviewer.

28.2.2.3 Lesson 3: Tactical PSYOP TTP: Cognitive influence-analysis case review using sample materials

Concept. Tactical PSYOP TTP: Cognitive influence-analysis case review using sample materials studies influence doctrine as audience analysis, message integrity, and ethics—not as manipulation technique.

Why it matters. Tactical PSYOP TTP matters in the **Cognitive Security and Influence Resilience** lane because information-integrity analysis and resilience education evidence must stay separate from judgment; treating resilience labels as permission to skip provenance review is a common failure.

Source support. Tactical PSYOP TTP: Cognitive influence-analysis case review using sample materials rests on [086, 2026]. The most specific cited work observes: A U.S. Use it for the working definition that **Tactical PSYOP TTP: Cognitive influence-analysis case review using sample materials** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Ground **Tactical PSYOP TTP** in the evidence the row cites. [086, 2026] A U.S. military field manual, FM 3-05.302, providing doctrine for tactical psychological operations at the unit level. The roughly 255-page document covers the organization of these units,

command relationships when supporting joint forces, a multi-phase product development and assessment process, and how intelligence supports such operations. It serves as a comprehensive training and reference document for personnel involved in tactical influence operations. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Tactical PSYOP TTP**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Tactical PSYOP TTP**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Tactical PSYOP TTP** work as a **narrative-risk and resilience map** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Tactical PSYOP TTP**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **Tactical PSYOP TTP** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

28.2.2.4 Lesson 4: FM 3-05 301: Cognitive influence-analysis case review using sample materials

Concept. FM 3-05 301: Cognitive influence-analysis case review using sample materials studies influence doctrine as audience analysis, message integrity, and ethics—not as manipulation technique.

Why it matters. FM 3-05 301: Cognitive influence-analysis case review using sample materials connects classroom vocabulary to Cognitive Security and Influence Resilience practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. FM 3-05 301: Cognitive influence-analysis case review using sample materials rests on [087, 2026]. Its anchor reference records: … Use it for fixing what **FM 3-05 301: Cognitive influence-analysis case review using sample materials** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **FM 3-05 301: Cognitive influence-analysis case review using sample materials**, work from the cited evidence behind this row. [087, 2026] … Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **FM 3-05 301**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **FM 3-05 301**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **FM 3-05 301: Cognitive influence-analysis case review using sample materials** work as a **narrative-risk and resilience map** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **FM 3-05 301: Cognitive influence-analysis case review using sample materials**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Apply this module's safe boundary for **FM 3-05 301: Cognitive influence-analysis case review using sample materials** to another artifact while keeping information-integrity analysis and resilience education and reviewer ownership explicit.

28.2.2.5 Lesson 5: Target Audience Analysis (TAA) and Susceptibility Mapping

Concept. Target Audience Analysis (TAA) and Susceptibility Mapping applies Target, Audience, Analysis within Cognitive Security and Influence Resilience: learners use separate analysis of influence from persuasion design and information-integrity analysis and resilience education evidence before any judgment moves forward.

Why it matters. Target Audience Analysis (TAA) matters in the **Cognitive Security and Influence Resilience** lane because information-integrity analysis and resilience education evidence must stay separate from judgment; counter-messaging as manipulation is a common failure.

Source support. Target Audience Analysis (TAA) and Susceptibility Mapping rests on [302, 2026] and [297, 2026]. The closest source to this row notes: The official "About Us" page of the National Geospatial-Intelligence Agency (NGA), a U.S. Use them for pinning down the scope of **Target Audience Analysis (TAA) and Susceptibility Mapping**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Target Audience Analysis (TAA)**, work from the cited evidence behind this row. [302, 2026] The official "About Us" page of the National Geospatial-Intelligence Agency (NGA), a U.S. Department of Defense and intelligence community organization. It describes NGA's mission of delivering geospatial intelligence, or GEOINT, to support military operations, policymakers, and first responders, spanning imagery analysis, mapping, geodesy, and navigation safety. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Target Audience Analysis (TAA)**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must name the source descriptor, the bounded claim about **Target Audience Analysis and Susceptibility**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Target Audience Analysis (TAA)** work as a **narrative-risk and resilience map** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that Target Audience Analysis (TAA) and Susceptibility Mapping replaces human review whenever evidence looks plausible.

Transfer task. Transfer **Target Audience Analysis (TAA)** to a second module by preserving information-integrity analysis and resilience education, changing the source evidence, and naming a new reviewer.

28.2.2.6 Lesson 6: PSYOP in Full-Spectrum Operations: Cognitive influence-analysis case review using sample materials

Concept. PSYOP in Full-Spectrum Operations: Cognitive influence-analysis case review using sample materials studies influence doctrine as audience analysis, message integrity, and ethics—not as manipulation technique.

Why it matters. PSYOP in Full-Spectrum Operations connects classroom vocabulary to Cognitive Security and Influence Resilience practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. PSYOP in Full-Spectrum Operations: Cognitive influence-analysis case review using sample materials rests on [086, 2026]. Its anchor reference records: The roughly 255-page document covers the organization of these units, command relationships when supporting joint forces, a multi-phase product development and assessment process, and how intelligence supports such operations. Use it for the working definition that **PSYOP in Full-Spectrum Operations: Cognitive influence-analysis case review using sample materials** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **PSYOP in Full-Spectrum Operations**, work from the cited evidence behind this row. [086, 2026] A U.S. military field manual, FM 3-05.302, providing doctrine for tactical psychological operations at the unit level. The roughly 255-page document covers the organization of these units, command relationships when supporting joint forces, a multi-phase product development and assessment process, and how intelligence supports such operations. It serves as a comprehensive training and reference document for personnel involved in tactical influence operations. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **PSYOP in Full-Spectrum Operations**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **PSYOP in Full-Spectrum Operations**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and

the reviewer accountable for correction. Shape **PSYOP in Full-Spectrum Operations** work as a **narrative-risk and resilience map** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **PSYOP in Full-Spectrum Operations**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Transfer **PSYOP in Full-Spectrum Operations** from this module to a second motif by preserving information-integrity analysis and resilience education, replacing action with audit, and naming the blocked use.

28.2.2.7 Lesson 7: Leaflets, Loudspeakers, and Digital Media: Product Development and Dissemination Concept. Leaflets, Loudspeakers, and Digital Media: Product Development and Dissemination applies Leaflets, Loudspeakers, Digital within Cognitive Security and Influence Resilience: learners use separate analysis of influence from persuasion design and information-integrity analysis and resilience education evidence before any judgment moves forward.

Why it matters. Leaflets, Loudspeakers, and Digital Media matters in the **Cognitive Security and Influence Resilience** lane because information-integrity analysis and resilience education evidence must stay separate from judgment; counter-messaging as manipulation is a common failure.

Source support. Leaflets, Loudspeakers, and Digital Media: Product Development and Dissemination rests on [308, 2026] and [311, 2026]. The most specific cited work observes: An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. Use them for fixing what **Leaflets, Loudspeakers, and Digital Media: Product Development and Dissemination** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Ground **Leaflets, Loudspeakers, and Digital Media** in the evidence the row cites. [308, 2026] An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure. [311, 2026] An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Leaflets, Loudspeakers, and Digital Media**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must name the source descriptor, the bounded claim about **Leaflets Loudspeakers and Digital Media**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Leaflets, Loudspeakers, and Digital Media** work as a **narrative-risk and resilience map** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that Leaflets, Loudspeakers, and Digital Media: Product Development and Dissemination is optional whenever separate analysis of influence from persuasion design feels inconvenient.

Transfer task. Transfer **Leaflets, Loudspeakers, and Digital Media** to a second module by preserving information-integrity analysis and resilience education, changing the source evidence, and naming a new reviewer.

28.2.3 PSYOP and MISO Doctrine worked safe example: synthetic inputs, evidence, and review

Worked example: a sample public-library class evaluates a synthetic rumor about a community service and compares transparent correction options. [238, 2026]; [239, 2026].

Triangulation anchors. In module 18's worked-example section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **information-integrity and influence analysis**. Learners use a **narrative-risk and resilience map** and keep this boundary visible: No covert persuasion, microtargeting, manipulation, or campaign design.

Frame. The classroom question centers on **Cognitive influence-analysis case review using sample materials**. Excluded actions stay explicit, and the **Cognitive-Resilience Lens** planning question is: How does the module protect autonomy, attention, trust, and decision quality without designing persuasion?

Inputs. For the **Cognitive influence-analysis case review using sample materials** scenario, use sample posts, source timestamps, public-service facts, and a media-literacy rubric. The Cognitive-Resilience Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Cognitive influence-analysis case review using sample materials**, students trace narrative provenance, separate observation from attribution, name audience harms, and design a transparent lesson. Pause whenever an inference about Cognitive influence-analysis case review using sample materials appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Cognitive influence-analysis case review using sample materials** classroom scenario; unit artifact = narrative-risk and resilience map; evidence = allowed inputs; method = information-integrity analysis and resilience education; output = a narrative-risk map with caveats, response options, and no microtargeted persuasion; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Cognitive influence-analysis case review using sample materials** as "Cognitive-Resilience Lens confirms it" is not enough. The revision ties the claim to information-integrity analysis and resilience education, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Cognitive influence-analysis case review using sample materials** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

28.2.4 PSYOP and MISO Doctrine practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Cognitive-Resilience Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2**.

Triangulation anchors. In module 18's practice-sequence section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Cognitive influence-analysis case review using sample materials, Military Information Support Operations: JP 3-13.2, Tactical PSYOP TTP: Cognitive influence-analysis case review using sample materials; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Cognitive Security and Influence Resilience** lane.
2. Frame	Answer the lens question: How does the module protect autonomy, attention, trust, and decision quality without designing persuasion?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Cognitive influence-analysis case review using sample materials: narrative-risk map with provenance, uncertainty, audience harms, and response options.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the narrative-risk and resilience map fields for Cognitive influence-analysis case review using sample materials.	Unit profile note.	Evidence artifacts include narrative provenance chain, audience-harm note.
4. Challenge	Test the misconception that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.	Failure-mode note.	The artifact applies the key distinction: separate analysis of influence from persuasion design.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

28.2.4.1 PSYOP and MISO Doctrine instructor notes: source reasoning, review points, and studio focus Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2**. [238, 2026]; [239, 2026].

28.2.4.2 PSYOP and MISO Doctrine extension exercise: peer validation and refresh trigger review **Evidence anchor.** Section 28; [238, 2026].

Have learners swap artifacts and apply the **Cognitive-Resilience Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2**.

28.2.5 PSYOP and MISO Doctrine knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 28; [238, 2026].

1. Explain how **Cognitive influence-analysis case review using sample materials** is defined here; name the source descriptor that supports the definition.
2. Contrast **Cognitive influence-analysis case review using sample materials** with **Military Information Support Operations: JP 3-13.2** using the **Cognitive-Resilience Lens** artifact fields.
3. Identify one failure mode from the **Cognitive Security and Influence Resilience** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which response informs people without crossing into MISO-style manipulation or unverified attribution?
5. Correct this misconception: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

28.2.5.1 PSYOP and MISO Doctrine answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Cognitive influence-analysis case review using sample materials** without source evidence, uncertainty, or a safe transfer task.

28.3 PSYOP and MISO Doctrine assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 28; [238, 2026].

28.3.1 PSYOP and MISO Doctrine evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 28; [238, 2026].

28.3.2 PSYOP and MISO Doctrine transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 28; [238, 2026].

28.3.2.1 PSYOP and MISO Doctrine lineage and source tradition: profile, concepts, and first anchors This sits in the **Cognitive Security and Influence Resilience** lineage: protecting attention, belief formation, and decision quality without turning resilience education into manipulation. [238, 2026]; [239, 2026].

28.3.2.2 PSYOP and MISO Doctrine working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 28; [238, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2**, with provenance and reviewability throughout.

28.3.2.3 PSYOP and MISO Doctrine knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [238, 2026]; [239, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

28.3.2.4 PSYOP and MISO Doctrine transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 28; [238, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2**.
- **Evidence contract:** keep the **Cognitive Security and Influence Resilience** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

28.3.2.5 PSYOP and MISO Doctrine profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 28; [238, 2026].

The matched profile emphasizes protecting attention, belief formation, and decision quality without turning resilience education into manipulation. The method stack is claim decomposition, narrative provenance, inoculation framing, bias checks, audience-risk review, and after-action learning; the local topic cluster is **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2**.

28.3.3 PSYOP and MISO Doctrine evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 28; [238, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Cognitive Security and Influence Resilience** profile tells reviewers what evidence is strong enough for the module artifact built around **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2**.

28.3.3.1 PSYOP and MISO Doctrine guide source spine: inherited keys and local citation roles Primary guide citations: [238, 2026]; [239, 2026]; [242, 2026]; [276, 2026]; [277, 2026]; [284, 2026]; [288, 2026]; [289, 2026]; [293, 2026]; [083, 2026]; [084, 2026]; [085, 2026]; [086, 2026]; [087, 2026]; [302, 2026]; [297, 2026]; [308, 2026]; [311, 2026].

28.3.3.2 PSYOP and MISO Doctrine verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [238, 2026]; [239, 2026].

Tier	What counts	How it is used
Source guide	[238, 2026]; [239, 2026]; [242, 2026]; [276, 2026]; [277, 2026]; [284, 2026]; [288, 2026]; [289, 2026]; [293, 2026]; [083, 2026]; [084, 2026]; [085, 2026]; [086, 2026]; [087, 2026]; [302, 2026]; [297, 2026]; [308, 2026]; [311, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 18's source-canon section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2** and [238, 2026]; [239, 2026], but only directly verified source URLs are encoded as citations.

28.3.3.3 PSYOP and MISO Doctrine intelligence practice lens: evidence artifact and safety check Practice lens: **Cognitive-Resilience Lens** for **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2**. [238, 2026]; [239, 2026].

Planning question: How does the module protect autonomy, attention, trust, and decision quality without designing persuasion?

Evidence artifact: narrative-risk map with provenance, uncertainty, audience harms, and response options.

Validation rule: distinguish observation, attribution, impact assessment, and resilience response. Applied to **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2**.

Handoff contract: handoff supports transparency, education, and resilience, not microtargeted influence or deception.

Safety check: exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning.

28.3.3.4 PSYOP and MISO Doctrine runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 28; [238, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	18.99	18.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind PSYOP and MISO Doctrine to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Bounded autonomy, procurement, incident-response, and assurance studio	18.101	18.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for PSYOP and MISO Doctrine	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Model-card, recoverability, retention, and learner-support evidence package	18.102	18.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for PSYOP and MISO Doctrine	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Cognitive influence-analysis case review using sample materials	18.1	18.1 source title transformed into safe curriculum treatment; original: Joint PSYOP Doctrine: JP 3-53 (1996 and 2003)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Military Information Support Operations (MISO): JP 3-13.2	18.2	18.2 Military Information Support Operations (MISO): JP 3-13.2	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Cognitive influence-analysis case review using sample materials	18.3	18.3 source title transformed into safe curriculum treatment; original: Tactical PSYOP TTP: FM 3-05.302	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Cognitive influence-analysis case review using sample materials	18.4	18.4 source title transformed into safe curriculum treatment; original: FM 3-05.301: PSYOP Process Tactics and Techniques	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Target Audience Analysis (TAA) and Susceptibility Mapping	18.5	18.5 Target Audience Analysis (TAA) and Susceptibility Mapping	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Cognitive influence-analysis case review using sample materials	18.6	18.6 source title transformed into safe curriculum treatment; original: PSYOP in Full-Spectrum Operations: Themes and Objectives	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Leaflets, Loudspeakers, and Digital Media: Product Development and Dissemination	18.7	18.7 Leaflets, Loudspeakers, and Digital Media: Product Development and Dissemination	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning

28.3.3.5 PSYOP and MISO Doctrine reusable subsection contract: topic rows, artifacts, and safety duties **Evidence anchor.** Section 28; [238, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Cognitive influence-analysis case review using sample materials	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Military Information Support Operations (MISO): JP 3-13.2	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Tactical PSYOP TTP: Cognitive influence-analysis case review using sample materials	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
FM 3-05 301: Cognitive influence-analysis case review using sample materials	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Target Audience Analysis (TAA) and Susceptibility Mapping	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
PSYOP in Full-Spectrum Operations: Cognitive influence-analysis case review using sample materials	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Leaflets, Loudspeakers, and Digital Media: Product Development and Dissemination	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning

28.3.3.6 PSYOP and MISO Doctrine annotated source ledger: real titles and local contribution Each source cited by this **Cognitive Security and Influence Resilience** module is paired below with its real title and a one-line note on what it contributes to **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2**.

Source	Cited work	What it contributes	Status
[238, 2026]	Recommendation on the Ethics of Artificial Intelligence	The official UNESCO page for the Recommendation on the Ethics of Artificial Intelligence, the first global standard-setting instrument on AI ethics, adopted in 2021 and applicable to all 194 member states. It outlines four core values, including human rights protection and environmental flourishing, and ten guiding principles such as proportionality, privacy, transparency, and fairness.	verified source-guide
[239, 2026]	Digital Space and Human Rights	Official OHCHR digital rights portal.	original source-guide
[242, 2026]	Guidance for Generative AI in Education and Research	Official UNESCO generative AI education guidance.	original source-guide
[276, 2026]	What is a Data Protection Impact Assessment and When Is This Mandatory?	A European Data Protection Board FAQ page, part of its data protection guide for small businesses, explaining Data Protection Impact Assessments (DPIAs) and when they are mandatory. It describes a DPIA as a written assessment of the impact of a planned processing operation, required when processing poses high risks to individuals' rights.	verified source-guide
[277, 2026]	Endorsed WP29 Guidelines	This is a European Data Protection Board webpage listing guidelines and documents originating from the Article 29 Working Party that the EDPB endorsed at its first plenary meeting. The catalogued materials relate to the GDPR and cover topics such as consent and transparency, data breach notification, automated decision-making and profiling, data protection impact assessments, data protection officers, and binding corporate rules.	verified source-guide
[284, 2026]	Verifiable Credential Data Integrity 1.0	The W3C Recommendation for Verifiable Credential Data Integrity 1.0, published May 2025, defining mechanisms for ensuring the authenticity and integrity of verifiable credentials using cryptographic proofs. It specifies a process of data transformation, hashing, and proof generation, and a corresponding verification procedure, along with a proof data model containing properties such as type, verification method, purpose, and proof value.	verified source-guide
[288, 2026]	Algorithmic Transparency Recording Standard Hub	A GOV.UK collection page serving as the hub for the UK Algorithmic Transparency Recording Standard (ATRS), maintained by the Government Digital Service. It provides a standardized template for documenting public-sector use of algorithmic tools, completion guidance, policy on scope and compliance, and a searchable repository of published transparency records.	verified source-guide

Source	Cited work	What it contributes	Status
[289, 2026]	Guidance for Organisations Using the Algorithmic Transparency Recording Standard	This is a GOV.UK guidance page published by the Government Digital Service that instructs public sector organizations on completing the Algorithmic Transparency Recording Standard (ATRS) template and publishing their records to the GOV.UK repository. It applies both to central government bodies required to publish under mandatory policy and to other public sector bodies doing so voluntarily.	verified source-guide
[293, 2026]	Inventory of NARA Artificial Intelligence (AI) Use Cases	The National Archives and Records Administration (NARA) official inventory of its artificial intelligence use cases, documenting 14 projects across deployed, pilot, and planned stages. Deployed efforts include workplace productivity tools, automated tagging for museum experiences, and historical record retrieval, while pilots cover PII detection and redaction, semantic search, and metadata generation, and planned work targets FOIA processing and public search.	verified source-guide
[083, 2026]	JP 3-53, "Doctrine for Joint Psychological Operations"	Joint Publication 3-53, the US Department of Defense joint doctrine for psychological operations. It establishes organizational structure, command relationships, planning processes, and approval authorities for integrating psychological operations into joint military campaigns and peacetime activities.	verified source-guide
[084, 2026]	JP 3-53 Doctrine for Joint Psychological Operations	Joint Publication 3-53, Doctrine for Joint Psychological Operations (Joint Chiefs of Staff, 10 July 1996). This US military doctrine document establishes the doctrinal basis for planning and conducting psychological operations in support of joint military operations.	verified source-guide
[085, 2026]	Military Information Support Operations	It sets forth joint doctrine to govern the activities and performance of the Armed Forces.	original source-guide
[086, 2026]	Tactical Psychological Operations Manual / PDF / Computers	A U.S. military field manual, FM 3-05.302, providing doctrine for tactical psychological operations at the unit level. The roughly 255-page document covers the organization of these units, command relationships when supporting joint forces, a multi-phase product development and assessment process, and how intelligence supports such operations. It serves as a comprehensive training and reference document for personnel involved in tactical influence operations.	verified source-guide context; do not use as primary analytic support
[087, 2026]	FM 3-05.301 Psychological Operations Process Tactics, Techniques	…	original source-guide

Source	Cited work	What it contributes	Status
[302, 2026]	National Geospatial-Intelligence Agency About Us	The official "About Us" page of the National Geospatial-Intelligence Agency (NGA), a U.S. Department of Defense and intelligence community organization. It describes NGA's mission of delivering geospatial intelligence, or GEOINT, to support military operations, policymakers, and first responders, spanning imagery analysis, mapping, geodesy, and navigation safety.	verified source-guide
[297, 2026]	Intelligence Community Directive 203: Analytic Standards	Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products.	original source-guide
[308, 2026]	Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure	An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure.	verified source-guide
[311, 2026]	Countering Information Threats	An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering.	verified source-guide

Where this sits. This module's overview is Section 28; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

28.3.4 PSYOP and MISO Doctrine governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 28; [238, 2026].

28.3.5 PSYOP and MISO Doctrine analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 18's governance-boundary section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Research lane: **Cognitive Security and Influence Resilience** for **Cognitive influence-analysis case review using sample materials; Military Information Support Operations (MISO): JP 3-13.2**. [238, 2026]; [239, 2026].
Curriculum topic spine: Cognitive influence-analysis case review using sample materials, **Military Information Support Operations (MISO): JP 3-13.2**, **Tactical PSYOP TTP: Cognitive influence-analysis case review using sample materials**. **Verified anchor cluster:** [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]; [OECD, 2026c]; [for Security Policy, 2025]; [Community, 2020a].
Conceptual depth: protecting attention, belief formation, and decision quality without turning resilience education into manipulation.
Method stack: claim decomposition, narrative provenance, inoculation framing, bias checks, audience-risk review, and after-action learning.
Composability contract: separate descriptive analysis, normative assessment, response options, and protected-audience considerations.
Known failure modes: counter-messaging as manipulation, overclaiming intent, pathologizing audiences, and collapsing uncertainty into moral certainty.
Defensive boundary: practice uses benign simulations and resilience education; it does not create persuasion campaigns, impersonation, or deception plans. Applied to **Cognitive influence-analysis case review using sample materials; Military Information Support Operations (MISO): JP 3-13.2**.

Anchor	Why it matters here
[Cybersecurity and Agency, 2024b]	Official CISA guidance on foreign influence operations targeting critical infrastructure. Checked as of 2026-05-21; role: source_quality_anchor.
[Organization, 2026b]	Official NATO counter-information-threat guidance. Checked as of 2026-05-21; role: source_quality_anchor.
[Cybersecurity and Agency, 2026b]	Official CISA election-security source for public-resilience, foreign-influence awareness, rumor control, and defensive communication framing. Checked as of 2026-05-21; role: curriculum_anchor.
[Organization, 2026c]	Official NATO source for hybrid-threat resilience across cyber, information, economic, political, and military pressure. Checked as of 2026-05-21; role: curriculum_anchor.
[OECD, 2026c]	Official OECD policy source for information integrity, governance responses, public trust, and democratic resilience. Checked as of 2026-05-21; role: curriculum_anchor.
[for Security Policy, 2025]	Policy-scholarship source for cognitive security, information literacy, critical thinking, and whole-of-society resilience. Checked as of 2026-05-21; role: curriculum_anchor.
[Community, 2020a]	Official IC framework for AI goals, authorities, human judgment, bias mitigation, testing, documentation, explainability, and review. Checked as of 2026-05-21; role: curriculum_anchor.

28.3.5.1 PSYOP and MISO Doctrine evidence standard and citation floor: source families and discovery limits Official guidance supplies governance, safety, and legal constraints for the **Cognitive Security and Influence Resilience** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [238, 2026]; [239, 2026].

28.3.6 PSYOP and MISO Doctrine agentic boundary: assist, approve, block, and record

Evidence anchor. Section 28; [238, 2026].
AGEINT translation is bounded by the **Cognitive Security and Influence Resilience** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2**.

28.3.6.1 PSYOP and MISO Doctrine permitted defensive utility: curriculum uses and safe outputs **Evidence anchor.** Section 28; [238, 2026].
The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2**.

28.3.6.2 PSYOP and MISO Doctrine excluded operational boundary: blocked actions and stop rules Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [238, 2026]; [239, 2026] and **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

28.3.7 PSYOP and MISO Doctrine governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 28; [238, 2026].
Governance is practiced as a gate on the **Cognitive Security and Influence Resilience** lane. Learners use the **Cognitive-Resilience Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2**.

28.3.7.1 PSYOP and MISO Doctrine governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [238, 2026]; [239, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Cognitive Security and Influence Resilience** failure modes and the **Cognitive-Resilience Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

28.3.7.2 PSYOP and MISO Doctrine evidence package handoff: appendices, records, and reuse **Evidence anchor.** Section 28; [238, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Cognitive-Resilience Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2**.

28.3.7.3 PSYOP and MISO Doctrine current-source assurance: verified anchors and local artifact fit The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2**. [238, 2026]; [239, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_cisa_foreign_influence` for **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2**?	Preparing for and Mitigating Foreign Influence Operations; lane `source_quality_spine`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official CISA guidance on foreign influence operations targeting critical infrastructure.
What does the module inherit from `official_nato_counter_information_threats` for **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2**?	Countering Information Threats; lane `source_quality_spine`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official NATO counter-information-threat guidance.
What does the module inherit from `official_cisa_election_security_influence` for **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2**?	Election Security; lane `cognitive_influence_security`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official CISA election-security source for public-resilience, foreign-influence awareness, rumor control, and defensive communication framing.
What does the module inherit from `official_nato_hybrid_threats` for **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2**?	Countering Hybrid Threats; lane `cognitive_influence_security`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official NATO source for hybrid-threat resilience across cyber, information, economic, political, and military pressure.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 28; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

28.3.8 PSYOP and MISO Doctrine assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 28; [238, 2026].

28.3.9 PSYOP and MISO Doctrine assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 28; [238, 2026].

28.3.9.1 PSYOP and MISO Doctrine capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2** and [238, 2026]; [239, 2026].

28.3.9.2 PSYOP and MISO Doctrine instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2** and [238, 2026]; [239, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

28.3.9.3 PSYOP and MISO Doctrine assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Cognitive influence-analysis case review using sample materials	Completed **narrative-risk map with provenance, uncertainty, audience harms, and response options** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Military Information Support Operations (MISO): JP 3-13.2	Completed **narrative-risk map with provenance, uncertainty, audience harms, and response options** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Tactical PSYOP TTP: Cognitive influence-analysis case review using sample materials	Completed **narrative-risk map with provenance, uncertainty, audience harms, and response options** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

28.3.10 PSYOP and MISO Doctrine refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [238, 2026]; [239, 2026] and **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2**.

28.3.10.1 PSYOP and MISO Doctrine refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2**. The local signals begin with [238, 2026]; [239, 2026].

28.3.10.2 PSYOP and MISO Doctrine claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2**, and the source spine for these checks begins with [238, 2026]; [239, 2026].

28.3.11 PSYOP and MISO Doctrine reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [238, 2026]; [239, 2026].

Triangulation anchors. In module 18's review-checklist section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2**. [238, 2026]; [239, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

28.3.12 PSYOP and MISO Doctrine learning-path links: module map, overview, and curriculum atlas

These links keep **Cognitive influence-analysis case review using sample materials; Military Information Support Operations: JP 3-13.2** paired with the orientation atlas, the parent unit, and the previous and next modules, so a reader can trace which claims and caveats are inherited rather than re-derived here. Anchored at [238, 2026]; [239, 2026].

Section 2, Section 27, Section 29

29 Active Measures and Disinformation

29.0.1 Active Measures and Disinformation figures and course links: visual evidence, source flow, and navigation

The module uses Figure 67 and Figure 64 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 27, Section 28, Section 30.
This module teaches the **Cognitive Security and Influence Resilience** lane through a bounded, source-backed coursebook chapter. [238, 2026]; [239, 2026].

29.1 Cognitive Security and Influence Resilience frame for Active Measures and Disinformation: source context, topic focus, and reader task

Evidence anchor. Section 29; [238, 2026].

29.1.1 Active Measures and Disinformation orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 29; [238, 2026].

29.1.2 Active Measures and Disinformation conceptual primer: source context, core model, and reader task

This chapter teaches cognitive security as protection of attention, trust, memory, and decision quality without creating manipulation. The chapter uses **Cognitive-Resilience Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**.
The central distinction is to separate analysis of influence from persuasion design. Core topics include **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation; Declassified source-protection and institutional-control case study**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [238, 2026]; [239, 2026].
Learners move from vocabulary and the **Cognitive-Resilience Lens** distinction through topic lessons on **Cognitive influence-analysis case review using sample materials** with evidence and misconception checks, then assemble a **narrative-risk map with provenance, uncertainty, audience harms, and response options** with safety and rights gates.

29.1.3 Active Measures and Disinformation learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 29; [238, 2026].

- Connect **Cognitive influence-analysis case review using sample materials and Dezinformatsiya: Forgery, Front Organizations, Media Manipulation** to **Cognitive Security and Influence Resilience** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate analysis of influence from persuasion design; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as counter-messaging as manipulation, overclaiming intent, pathologizing audiences, and collapsing uncertainty into moral certainty, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: practice uses benign simulations and resilience education; it does not create persuasion campaigns, impersonation, or deception plans.

29.1.4 Active Measures and Disinformation core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 29; [238, 2026].

Term	Working definition
Narrative provenance	where a claim, frame, or story came from and how it spread
Prebunking	transparent education that helps people recognize misleading patterns before exposure
Audience harm	a privacy, dignity, autonomy, or trust risk for people receiving information
Attribution caution	the rule that intent and origin claims need strong evidence
Resilience response	a transparent education, correction, or process improvement that avoids manipulation
MISO boundary	the line between accountable public messaging analysis and covert influence design
Inoculation	building recognition of manipulation tactics without deploying persuasion against a population
Cognitive influence-analysis case review using…	Key terms: Cognitive, influence, analysis.
Dezinformatsiya: Forgery, Front Organizations,…	Key terms: Dezinformatsiya, Forgery, Front.

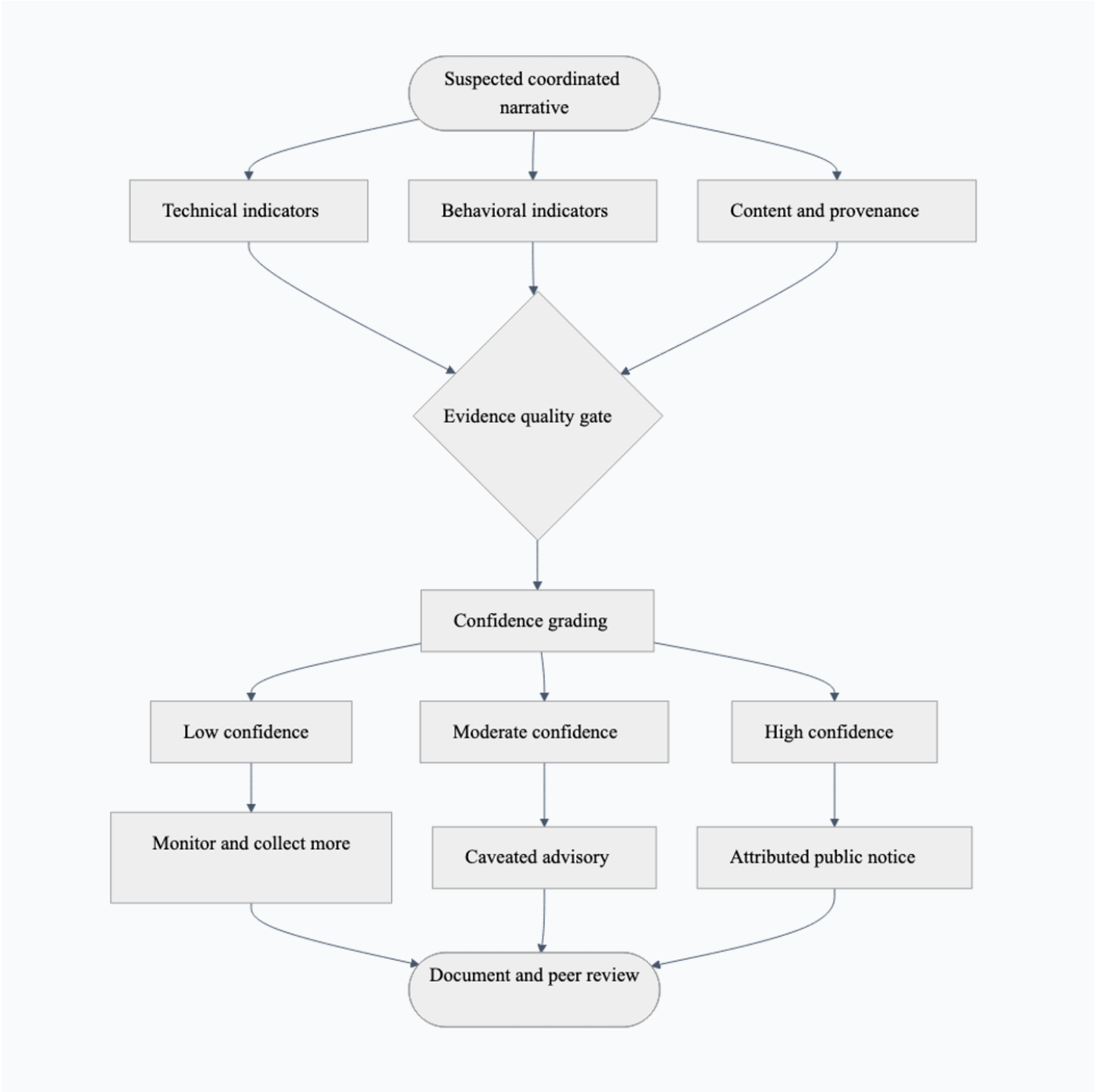


Figure 67: How analysts move a suspected influence narrative from raw signals through evidence gating to a graded, defensible attribution-confidence judgment. The captioned view belongs to the psychological operations and influence / active measures and disinformation section and should be read as a map of Suspected coordinated narrative, Technical indicators, Behavioral indicators, and Content and provenance, not as a capability score or live-task instruction.

29.2 Cognitive-Resilience Lens path for Active Measures and Disinformation: lesson cluster, safe artifact, and review

Evidence anchor. Section 29; [238, 2026].

29.2.1 Active Measures and Disinformation practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 29; [238, 2026].

29.2.2 Active Measures and Disinformation topic lessons: source-backed concepts and transfer tasks

This module builds cognitive security as protection of attention, trust, memory, and decision quality without creating manipulation. The sequence opens with **Cognitive influence-analysis case review using sample materials**, **Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**, **Declassified source-protection and institutional-control case study** and applies the **Cognitive-Resilience Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 64; module overview Section 29; curriculum atlas Section 2.

Triangulation anchors. In module 19's topic-lessons section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

29.2.2.1 Lesson 1: Cognitive influence-analysis case review using sample materials Concept. Cognitive influence-analysis case review using sample materials analyzes influence campaigns through provenance, audience harm, attribution caution, and transparent response options.

Why it matters. Analysts use **Cognitive influence-analysis case review** to separate analysis of influence from persuasion design. A defensible treatment names the judgment it enables for information-integrity analysis and resilience education review, the proof limit that treating resilience labels as permission to skip provenance review would otherwise hide, and the reviewer accountable for challenge.

Source support. Cognitive influence-analysis case review using sample materials rests on [088, 2026] and [089, 2026]. The closest source to this row notes: Department of State Bureau of Public Affairs report from October 1981, released under FOIA. Use them for the claim that **Cognitive influence-analysis case review using sample materials** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Cognitive influence-analysis case review**, work from the cited evidence behind this row. [088, 2026] A U.S. Department of State Bureau of Public Affairs report from October 1981, released under FOIA. It catalogs Soviet 'active measures' — the Soviet term for covert influence operations — including written disinformation, control of foreign media, use of front organizations, clandestine broadcasting, blackmail, and political influence operations. Specific cases include Soviet forgeries related to the 1979 Grand Mosque seizure and NATO theater nuclear force debates. [089, 2026] An article by Dennis Kux published in Parameters: Journal of the US Army War College (1985) and preserved in the CIA CREST archive. It defines and distinguishes Soviet 'disinformation' and 'active measures,' situating them within a spectrum of white, gray, and black foreign influence operations. Kux examines KGB front groups, agents of influence, forgeries, and the broader strategic goal of tarnishing Western governments while advancing Soviet foreign policy. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Cognitive influence-analysis case review**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Cognitive influence-analysis case review using**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Cognitive influence-analysis case review** work as a **narrative-risk and resilience map** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Cognitive influence-analysis case review**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Apply this module's safe boundary for **Cognitive influence-analysis case review** to another artifact while keeping information-integrity analysis and resilience education and reviewer ownership explicit.

29.2.2.2 Lesson 2: Dezinformatsiya: Forgery, Front Organizations, Media Manipulation Concept. Dezinformatsiya: Forgery, Front Organizations, Media Manipulation applies Dezinformatsiya, Forgery, Front within Cognitive Security and Influence Resilience: learners use separate analysis of influence from persuasion design and information-integrity analysis and resilience education evidence before any judgment moves forward.

Why it matters. Analysts use **Dezinformatsiya: Forgery, Front Organizations, Media Manipulation** to separate analysis of influence from persuasion design. A defensible treatment names the judgment it enables for information-integrity analysis and resilience education review, the proof limit that counter-messaging as manipulation would otherwise hide, and the reviewer accountable for challenge.

Source support. Dezinformatsiya: Forgery, Front Organizations, Media Manipulation rests on [090, 2026] and [091, 2026]. The closest source to this row notes: It explains the KGB's use of forgeries, disinformation, and front organizations to covertly influence foreign governments and publics, illustrating with the forged 1984 Olympic KKK leaflet operation designed to discourage participation in the Los Angeles Games. Use them for pinning down the scope of **Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Ground **Dezinformatsiya: Forgery, Front Organizations, Media Manipulation** in the evidence the row cites. [090, 2026] A CIA CREST record (October 1981, released March 2007) comprising a routing and record sheet from the PCS/PGLO office dated February 8, 1982, attached to the same Department of State Special Report No. 88 on Soviet active measures. The document is catalogued as an open-source CREST entry and captures the internal CIA circulation of the State Department's public report on Soviet forgery and disinformation operations. [091, 2026] A declassified-in-part 1986 CIA speech text on Soviet active measures, prepared by the Foreign Activities Branch, Third World Activities Division, Office of Soviet Analysis. It explains the KGB's use of forgeries, disinformation, and front organizations to covertly influence foreign governments and publics, illustrating with the forged 1984 Olympic KKK leaflet operation designed to discourage participation in the Los Angeles Games. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Dezinformatsiya**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must name the source descriptor, the bounded claim about **Dezinformatsiya**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Dezinformatsiya: Forgery, Front Organizations, Media Manipulation** work as a **narrative-risk and resilience map** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that Dezinformatsiya: Forgery, Front Organizations, Media Manipulation can be used while ignoring the rule to separate analysis of influence from persuasion design.

Transfer task. Transfer **Dezinformatsiya: Forgery, Front Organizations, Media Manipulation** to a second module by preserving information-integrity analysis and resilience education, changing the source evidence, and naming a new reviewer.

29.2.2.3 Lesson 3: Declassified source-protection and institutional-control case study **Concept. Declassified source-protection and institutional-control case study** studies the declassified record for institutional lessons about oversight, source protection, and limits on translating history into practice.

Why it matters. Analysts use **Declassified source-protection** to separate analysis of influence from persuasion design. A defensible treatment names the judgment it enables for information-integrity analysis and resilience education review, the proof limit that counter-messaging as manipulation would otherwise hide, and the reviewer accountable for challenge.

Source support. Declassified source-protection and institutional-control case study rests on [089, 2026]. The lead source's own note reads: An article by Dennis Kux published in Parameters: Journal of the US Army War College (1985) and preserved in the CIA CREST archive. Use it for the working definition that **Declassified source-protection and institutional-control case study** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Declassified source-protection**, reason from the sources cited in this row. [089, 2026] An article by Dennis Kux published in Parameters: Journal of the US Army War College (1985) and preserved in the CIA CREST archive. It defines and distinguishes Soviet 'disinformation' and 'active measures,' situating them within a spectrum of white, gray, and black foreign influence operations. Kux examines KGB front groups, agents of influence, forgeries, and the broader strategic goal of tarnishing Western governments while advancing Soviet foreign policy. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Declassified source-protection**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must cite the declassified source descriptor, the bounded lesson about **Declassified source-protection and institutional-control case**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape **Declassified source-protection** work as a **narrative-risk and resilience map** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Transfer **Declassified source-protection** from this module to a second motif by preserving information-integrity analysis and resilience education, replacing action with audit, and naming the blocked use.

29.2.2.4 Lesson 4: Historical Active Measures Campaigns: Cognitive influence-analysis case review using sample materials **Concept. Historical Active Measures Campaigns: Cognitive influence-analysis case review using sample materials** analyzes influence campaigns through provenance, audience harm, attribution caution, and transparent response options.

Why it matters. Analysts use **Historical Active Measures Campaigns** to separate analysis of influence from persuasion design. A defensible treatment names the judgment it enables for information-integrity analysis and resilience education review, the proof limit that treating resilience labels as permission to skip provenance review would otherwise hide, and the reviewer accountable for challenge.

Source support. Historical Active Measures Campaigns: Cognitive influence-analysis case review using sample materials rests on [091, 2026]. The lead source's own note reads: It explains the KGB's use of forgeries, disinformation, and front organizations to covertly influence foreign governments and publics, illustrating with the forged 1984 Olympic KKK leaflet operation designed to discourage participation in the Los Angeles Games. Use it for the working definition that **Historical Active Measures Campaigns: Cognitive influence-analysis case review using sample materials** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Read **Historical Active Measures Campaigns** against the works cited for this row. [091, 2026] A declassified-in-part 1986 CIA speech text on Soviet active measures, prepared by the Foreign Activities Branch, Third World Activities Division, Office of Soviet Analysis. It explains the KGB's use of forgeries, disinformation, and front organizations to covertly influence foreign governments and publics, illustrating with the forged 1984 Olympic KKK leaflet operation designed to discourage participation in the Los Angeles Games. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Historical Active Measures Campaigns**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Historical Active Measures Campaigns**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Historical Active Measures Campaigns** work as a **narrative-risk and resilience map** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Historical Active Measures Campaigns**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Transfer **Historical Active Measures Campaigns** from this module to a second motif by preserving information-integrity analysis and resilience education, replacing action with audit, and naming the blocked use.

29.2.2.5 Lesson 5: Russian Active Measures in the: Cognitive influence-analysis case review using sample materials **Concept. Russian Active Measures in the: Cognitive influence-analysis case review using sample materials** analyzes influence campaigns through provenance, audience harm, attribution caution, and transparent response options.

Why it matters. Russian Active Measures in the matters in the **Cognitive Security and Influence Resilience** lane because information-integrity analysis and resilience education evidence must stay separate from judgment; treating resilience labels as permission to skip provenance review is a common failure.

Source support. Russian Active Measures in the: Cognitive influence-analysis case review using sample materials rests on [092, 2026]. The most specific cited work observes: It examines the historical background of Soviet and Russian disinformation, including the concept of active measures, and how disinformation is woven into strategic narratives and diplomacy. Use it for the working definition that **Russian Active Measures in the: Cognitive influence-analysis case review using sample materials** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Russian Active Measures in the**, work from the cited evidence behind this row. [092, 2026] A March 2019 CREST (Centre for Research and Evidence on Security Threats) report titled "Russia and Disinformation: Maskirovka," prepared by scholars of Russian foreign and security policy using open-source and Russian-language primary material. It examines the historical background of Soviet and Russian disinformation, including the concept of active measures, and how disinformation is woven into strategic narratives and diplomacy. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Russian Active Measures in the**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Russian Active Measures**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Russian Active Measures in the** work as a **narrative-risk and resilience map** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Russian Active Measures in the**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **Russian Active Measures in the** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

29.2.2.6 Lesson 6: Chinese Information Operations: United Front Work Department Concept. Chinese Information Operations: United Front Work Department applies Chinese, Information, Operations within Cognitive Security and Influence Resilience: learners use separate analysis of influence from persuasion design and information-integrity analysis and resilience education evidence before any judgment moves forward.

Why it matters. Chinese Information Operations connects classroom vocabulary to Cognitive Security and Influence Resilience practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Chinese Information Operations: United Front Work Department rests on [308, 2026] and [311, 2026]. Its anchor reference records: It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering. Use them for pinning down the scope of **Chinese Information Operations: United Front Work Department**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Ground **Chinese Information Operations** in the evidence the row cites. [308, 2026] An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure. [311, 2026] An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Chinese Information Operations**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must name the source descriptor, the bounded claim about **Chinese Information Operations**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Chinese Information Operations** work as a **narrative-risk and resilience map** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that Chinese Information Operations: United Front Work Department can be used while ignoring the rule to separate analysis of influence from persuasion design.

Transfer task. Transfer **Chinese Information Operations** to a second module by preserving information-integrity analysis and resilience education, changing the source evidence, and naming a new reviewer.

29.2.2.7 Lesson 7: Deception, Disinformation, and Strategic Communications (NDU/Brown) Concept. Deception, Disinformation, and Strategic Communications (NDU/Brown) analyzes influence campaigns through provenance, audience harm, attribution caution, and transparent response options.

Why it matters. Without explicit treatment of **Deception, Disinformation, and Strategic Communications (NDU/Brown)**, counter-messaging as manipulation undermines information-integrity analysis and resilience education review; the lesson builds the habit to separate analysis of influence from persuasion design.

Source support. Deception, Disinformation, and Strategic Communications (NDU/Brown) rests on [093, 2026] and [094, 2026]. The closest source to this row notes: Lamb, 'Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference,' INSS Strategic Perspectives No. Use them for the claim that **Deception, Disinformation, and Strategic Communications (NDU/Brown)** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Ground **Deception, Disinformation, and Strategic Communications (NDU/Brown)** in the evidence the row cites. [093, 2026] Fletcher Schoen and Christopher J. Lamb, 'Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference,' INSS Strategic Perspectives No. 11 (NDU Press, June 2012). The study examines the U.S. Active Measures Working Group, a small interagency committee formed in the 1980s to expose and counter Soviet disinformation, and analyzes why it succeeded where most such groups fail. [094, 2026] Fletcher Schoen and Christopher J. Lamb, 'Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference,' INSS Strategic Perspectives No. 11 (NDU Press, June 2012). Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Deception, Disinformation, and Strategic Communications (NDU/Brown)**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must name the source descriptor, the bounded claim about **Deception Disinformation and Strategic Communications**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape this subject work as a **narrative-risk and resilience map** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that Deception, Disinformation, and Strategic Communications (NDU/Brown) is optional whenever separate analysis of influence from persuasion design feels inconvenient.

Transfer task. Transfer **Deception, Disinformation, and Strategic Communications (NDU/Brown)** to a second module by preserving information-integrity analysis and resilience education, changing the source evidence, and naming a new reviewer.

29.2.2.8 Lesson 8: AI-Driven Active Measures: Cognitive influence-analysis case review using sample materials Concept. AI-Driven Active Measures: Cognitive influence-analysis case review using sample materials compares resolution, accuracy, and temporal fitness before drawing a geospatial conclusion from imagery or map products.

Why it matters. Analysts use **AI-Driven Active Measures** to separate analysis of influence from persuasion design. A defensible treatment names the judgment it enables for information-integrity analysis and resilience education review, the proof limit that treating resilience labels as permission to skip provenance review would otherwise hide, and the reviewer accountable for challenge.

Source support. AI-Driven Active Measures: Cognitive influence-analysis case review using sample materials rests on [095, 2026] and [096, 2026]. The lead source's own note reads: A position paper (Stanford authors, ICLR 2026 workshop) arguing that AI research and development should prioritize cognitive security, defined as protecting human cognitive processes from hazardous influence. Use them for the claim that **AI-Driven Active Measures: Cognitive influence-analysis case review using sample materials** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **AI-Driven Active Measures**, work from the cited evidence behind this row. [095, 2026] This policy paper examines the emergence of cognitive security. [096, 2026] A position paper (Stanford authors, ICLR 2026 workshop) arguing that AI research and development should prioritize cognitive security, defined as protecting human cognitive processes from hazardous influence. It notes that generative AI systems increasingly designed to influence beliefs and behavior raise acute governance concerns, while research on these effects remains fragmented. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **AI-Driven Active Measures**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **AI-Driven Active Measures**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **AI-Driven Active Measures** work as a **narrative-risk and resilience map** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **AI-Driven Active Measures**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **AI-Driven Active Measures** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

29.2.2.9 Lesson 9: Countermeasures: Disinformation Detection and Response

Concept. Countermeasures: Disinformation Detection and Response analyzes influence campaigns through provenance, audience harm, attribution caution, and transparent response options.

Why it matters. Countermeasures: Disinformation Detection and Response matters in the **Cognitive Security and Influence Resilience** lane because information-integrity analysis and resilience education evidence must stay separate from judgment; counter-messaging as manipulation is a common failure.

Source support. Countermeasures: Disinformation Detection and Response rests on [092, 2026]. The most specific cited work observes: A March 2019 CREST (Centre for Research and Evidence on Security Threats) report titled "Russia and Disinformation: Maskirovka," prepared by scholars of Russian foreign and security policy using open-source and Russian-language primary material. Use it for the working definition that **Countermeasures: Disinformation Detection and Response** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Countermeasures: Disinformation Detection and Response**, work from the cited evidence behind this row. [092, 2026] A March 2019 CREST (Centre for Research and Evidence on Security Threats) report titled "Russia and Disinformation: Maskirovka," prepared by scholars of Russian foreign and security policy using open-source and Russian-language primary material. It examines the historical background of Soviet and Russian disinformation, including the concept of active measures, and how disinformation is woven into strategic narratives and diplomacy. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Countermeasures**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must name the source descriptor, the bounded claim about **Countermeasures**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Countermeasures: Disinformation Detection and Response** work as a **narrative-risk and resilience map** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that Countermeasures: Disinformation Detection and Response replaces human review whenever evidence looks plausible.

Transfer task. Transfer **Countermeasures: Disinformation Detection and Response** to a second module by preserving information-integrity analysis and resilience education, changing the source evidence, and naming a new reviewer.

29.2.3 Active Measures and Disinformation worked safe example: synthetic inputs, evidence, and review

Worked example: a sample public-library class evaluates a synthetic rumor about a community service and compares transparent correction options. [238, 2026]; [239, 2026].

Triangulation anchors. In module 19's worked-example section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **information-integrity and influence analysis**. Learners use a **narrative-risk and resilience map** and keep this boundary visible: No covert persuasion, microtargeting, manipulation, or campaign design.

Frame. The classroom question centers on **Cognitive influence-analysis case review using sample materials**. Excluded actions stay explicit, and the **Cognitive-Resilience Lens** planning question is: How does the module protect autonomy, attention, trust, and decision quality without designing persuasion?

Inputs. For the **Cognitive influence-analysis case review using sample materials** scenario, use sample posts, source timestamps, public-service facts, and a media-literacy rubric. The Cognitive-Resilience Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Cognitive influence-analysis case review using sample materials**, students trace narrative provenance, separate observation from attribution, name audience harms, and design a transparent lesson. Pause whenever an inference about Cognitive influence-analysis case review using sample materials appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Cognitive influence-analysis case review using sample materials** classroom scenario; unit artifact = narrative-risk and resilience map; evidence = allowed inputs; method = information-integrity analysis and resilience education; output = a narrative-risk map with caveats, response options, and no microtargeted persuasion; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Cognitive influence-analysis case review using sample materials** as "Cognitive-Resilience Lens confirms it" is not enough. The revision ties the claim to information-integrity analysis and resilience education, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Cognitive influence-analysis case review using sample materials** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

29.2.4 Active Measures and Disinformation practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Cognitive-Resilience Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**.

Triangulation anchors. In module 19's practice-sequence section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Cognitive influence-analysis case review using sample materials, Dezinformatsiya: Forgery, Front Organizations, Media Manipulation, Declassified source-protection and institutional-control case study; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Cognitive Security and Influence Resilience** lane.

Move	Learner action	Output	Check
2. Frame	Answer the lens question: How does the module protect autonomy, attention, trust, and decision quality without designing persuasion?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Cognitive influence-analysis case review using sample materials: narrative-risk map with provenance, uncertainty, audience harms, and response options.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the narrative-risk and resilience map fields for Cognitive influence-analysis case review using sample materials.	Unit profile note.	Evidence artifacts include narrative provenance chain, audience-harm note.
4. Challenge	Test the misconception that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.	Failure-mode note.	The artifact applies the key distinction: separate analysis of influence from persuasion design.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

29.2.4.1 Active Measures and Disinformation instructor notes: source reasoning, review points, and studio focus Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**. [238, 2026]; [239, 2026].

29.2.4.2 Active Measures and Disinformation extension exercise: peer validation and refresh trigger review **Evidence anchor.** Section 29; [238, 2026].

Have learners swap artifacts and apply the **Cognitive-Resilience Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**.

29.2.5 Active Measures and Disinformation knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 29; [238, 2026].

1. Explain how **Cognitive influence-analysis case review using sample materials** is defined here; name the source descriptor that supports the definition.
2. Contrast **Cognitive influence-analysis case review using sample materials** with **Dezinformatsiya: Forgery, Front Organizations, Media Manipulation** using the **Cognitive-Resilience Lens** artifact fields.
3. Identify one failure mode from the **Cognitive Security and Influence Resilience** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which response informs people without crossing into MISO-style manipulation or unverified attribution?
5. Correct this misconception: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

29.2.5.1 Active Measures and Disinformation answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Cognitive influence-analysis case review using sample materials** without source evidence, uncertainty, or a safe transfer task.

29.3 Active Measures and Disinformation assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 29; [238, 2026].

29.3.1 Active Measures and Disinformation evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 29; [238, 2026].

29.3.2 Active Measures and Disinformation transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 29; [238, 2026].

29.3.2.1 Active Measures and Disinformation lineage and source tradition: profile, concepts, and first anchors This sits in the **Cognitive Security and Influence Resilience** lineage: protecting attention, belief formation, and decision quality without turning resilience education into manipulation. [238, 2026]; [239, 2026].

29.3.2.2 Active Measures and Disinformation working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 29; [238, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**, with provenance and reviewability throughout.

29.3.2.3 Active Measures and Disinformation knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [238, 2026]; [239, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

29.3.2.4 Active Measures and Disinformation transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 29; [238, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**.
- **Evidence contract:** keep the **Cognitive Security and Influence Resilience** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

29.3.2.5 Active Measures and Disinformation profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 29; [238, 2026].

The matched profile emphasizes protecting attention, belief formation, and decision quality without turning resilience education into manipulation. The method stack is claim decomposition, narrative provenance, inoculation framing, bias checks, audience-risk review, and after-action learning; the local topic cluster is **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**.

29.3.3 Active Measures and Disinformation evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 29; [238, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Cognitive Security and Influence Resilience** profile tells reviewers what evidence is strong enough for the module artifact built around **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**.

29.3.3.1 Active Measures and Disinformation guide source spine: inherited keys and local citation roles Primary guide citations: [238, 2026]; [239, 2026]; [240, 2026]; [278, 2026]; [279, 2026]; [283, 2026]; [290, 2026]; [291, 2026]; [294, 2026]; [088, 2026]; [089, 2026]; [090, 2026]; [091, 2026]; [092, 2026]; [093, 2026]; [094, 2026]; [095, 2026]; [096, 2026]; [308, 2026]; [311, 2026].

29.3.3.2 Active Measures and Disinformation verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [238, 2026]; [239, 2026].

Tier	What counts	How it is used
Source guide	[238, 2026]; [239, 2026]; [240, 2026]; [278, 2026]; [279, 2026]; [283, 2026]; [290, 2026]; [291, 2026]; [294, 2026]; [088, 2026]; [089, 2026]; [090, 2026]; [091, 2026]; [092, 2026]; [093, 2026]; [094, 2026]; [095, 2026]; [096, 2026]; [308, 2026]; [311, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 19's source-canon section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation** and [238, 2026]; [239, 2026], but only directly verified source URLs are encoded as citations.

29.3.3.3 Active Measures and Disinformation intelligence practice lens: evidence artifact and safety check Practice lens: **Cognitive-Resilience Lens** for **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**. [238, 2026]; [239, 2026].

Planning question: How does the module protect autonomy, attention, trust, and decision quality without designing persuasion?

Evidence artifact: narrative-risk map with provenance, uncertainty, audience harms, and response options.

Validation rule: distinguish observation, attribution, impact assessment, and resilience response. Applied to **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**.

Handoff contract: handoff supports transparency, education, and resilience, not microtargeted influence or deception.

Safety check: exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning.

29.3.3.4 Active Measures and Disinformation runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 29; [238, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	19.99	19.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Active Measures and Disinformation to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Bounded autonomy, procurement, incident-response, and assurance studio	19.101	19.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Active Measures and Disinformation	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Model-card, recoverability, retention, and learner-support evidence package	19.102	19.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Active Measures and Disinformation	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Cognitive influence-analysis case review using sample materials	19.1	19.1 source title transformed into safe curriculum treatment; original: Soviet Active Measures: Definitions and Doctrine	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Dezinformatsiya: Forgery, Front Organizations, Media Manipulation	19.2	19.2 Dezinformatsiya: Forgery, Front Organizations, Media Manipulation	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Declassified source-protection and institutional-control case study	19.3	19.3 source title transformed into safe curriculum treatment; original: KGB Aktivnyye Meropriyatiya: Historical Organization	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Cognitive influence-analysis case review using sample materials	19.4	19.4 source title transformed into safe curriculum treatment; original: Historical Active Measures Campaigns: INFEKTION, RYAN, DENVER	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Cognitive influence-analysis case review using sample materials	19.5	19.5 source title transformed into safe curriculum treatment; original: Russian Active Measures in the Contemporary Era	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Chinese Information Operations: United Front Work Department	19.6	19.6 Chinese Information Operations: United Front Work Department	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Deception, Disinformation, and Strategic Communications (NDU/Brown)	19.7	19.7 Deception, Disinformation, and Strategic Communications (NDU/Brown)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Cognitive influence-analysis case review using sample materials	19.8	19.8 source title transformed into safe curriculum treatment; original: AI-Driven Active Measures: Synthetic Influence at Scale	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Countermeasures: Disinformation Detection and Response	19.9	19.9 Countermeasures: Disinformation Detection and Response	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning

29.3.3.5 Active Measures and Disinformation reusable subsection contract: topic rows, artifacts, and safety duties Evidence anchor. Section 29; [238, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Cognitive influence-analysis case review using sample materials	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Dezinformatsiya: Forgery, Front Organizations, Media Manipulation	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Declassified source-protection and institutional-control case study	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Historical Active Measures Campaigns: Cognitive influence-analysis case review using sample materials	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Russian Active Measures in the: Cognitive influence-analysis case review using sample materials	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning

Lesson topic	Practice lens	Evidence artifact	Safety check
Chinese Information Operations: United Front Work Department	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Deception, Disinformation, and Strategic Communications (NDU/Brown)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
AI-Driven Active Measures: Cognitive influence-analysis case review using sample materials	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Countermeasures: Disinformation Detection and Response	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning

29.3.3.6 Active Measures and Disinformation annotated source ledger: real titles and local contribution Each source cited by this **Cognitive Security and Influence Resilience** module is paired below with its real title and a one-line note on what it contributes to **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**.

Source	Cited work	What it contributes	Status
[238, 2026]	Recommendation on the Ethics of Artificial Intelligence	The official UNESCO page for the Recommendation on the Ethics of Artificial Intelligence, the first global standard-setting instrument on AI ethics, adopted in 2021 and applicable to all 194 member states. It outlines four core values, including human rights protection and environmental flourishing, and ten guiding principles such as proportionality, privacy, transparency, and fairness.	verified source-guide
[239, 2026]	Digital Space and Human Rights	Official OHCHR digital rights portal.	original source-guide
[240, 2026]	The Right to Privacy in the Digital Age	The Office of the High Commissioner for Human Rights (OHCHR) hub page on the right to privacy in the digital age. It addresses how data-intensive technologies, particularly artificial intelligence, create risks for privacy, autonomy, and human dignity, and curates international standards, reports, and expert consultations.	verified source-guide
[278, 2026]	Recommendation of the Council on Public Procurement	The OECD Recommendation of the Council on Public Procurement (OECD/LEGAL/0411), a legal instrument adopted by the OECD Council in 2015 on the proposal of the Public Governance Committee. It frames public procurement as a pillar of strategic governance and service delivery and sets out principles for governments to follow.	verified source-guide
[279, 2026]	Open Contracting Data Standard	The documentation homepage for the Open Contracting Data Standard, version 1.1.5, maintained by the Open Contracting Partnership to support disclosure of government contracting data across the procurement lifecycle. It provides a common data model spanning planning, tender, award, contract, and implementation stages, along with a primer, implementation guidance, technical schemas, and validation tooling.	verified source-guide

Source	Cited work	What it contributes	Status
[283, 2026]	Recommendation of the Council on Open Government	An OECD legal instrument document reproducing the Recommendation of the Council on Open Government (OECD/LEGAL/0438), adopted on 14 December 2017. It defines open government as a culture of governance promoting transparency, integrity, accountability, and stakeholder participation in support of democracy and inclusive growth.	verified source-guide
[290, 2026]	NIST SP 800-218A: Secure Software Development Practices for Generative AI and Dual-Use Foundation Models	NIST Special Publication 800-218A (July 2024), which augments the Secure Software Development Framework with practices specific to AI model development across the software lifecycle. Produced in response to Executive Order 14110, it addresses AI model producers, developers building on those models, and acquirers of AI systems, and is designed to be used alongside NIST SP 800-218.	verified source-guide
[291, 2026]	Revised 508 Standards and 255 Guidelines	Official documentation from the U.S. Access Board on the Revised 508 Standards and 255 Guidelines for information and communication technology accessibility. It establishes mandatory accessibility requirements for federal agencies and voluntary guidelines for telecommunications manufacturers, covering hardware, software, websites, electronic documents, and support services.	verified source-guide
[294, 2026]	M-25-21: Accelerating Federal Use of AI through Innovation, Governance, and Public Trust	An April 2025 Office of Management and Budget memorandum (M-25-21) directing executive branch agencies on federal use of artificial intelligence. Issued under Executive Order 14179, it instructs agencies to accelerate adoption of AI to improve public services and government efficiency while maintaining safeguards for civil rights, civil liberties, and privacy.	verified source-guide
[088, 2026]	SOVIET 'ACTIVE MEASURES' FORGERY, DISINFORMATION, POLITICAL OPERATIONS	A U.S. Department of State Bureau of Public Affairs report from October 1981, released under FOIA. It catalogs Soviet 'active measures' — the Soviet term for covert influence operations — including written disinformation, control of foreign media, use of front organizations, clandestine broadcasting, blackmail, and political influence operations. Specific cases include Soviet forgeries related to the 1979 Grand Mosque seizure and NATO theater nuclear force debates.	verified source-guide

Source	Cited work	What it contributes	Status
[089, 2026]	SOVIET ACTIVE MEASURES AND DISINFORMATION: OVERVIEW AND ASSESSMENT	An article by Dennis Kux published in Parameters: Journal of the US Army War College (1985) and preserved in the CIA CREST archive. It defines and distinguishes Soviet 'disinformation' and 'active measures,' situating them within a spectrum of white, gray, and black foreign influence operations. Kux examines KGB front groups, agents of influence, forgeries, and the broader strategic goal of tarnishing Western governments while advancing Soviet foreign policy.	verified source-guide
[090, 2026]	"SOVIET ACTIVE MEASURES: FORGERY, DISINFORMATION, POLITICAL OPERATIONS"	A CIA CREST record (October 1981, released March 2007) comprising a routing and record sheet from the PCS/PGLO office dated February 8, 1982, attached to the same Department of State Special Report No. 88 on Soviet active measures. The document is catalogued as an open-source CREST entry and captures the internal CIA circulation of the State Department's public report on Soviet forgery and disinformation operations.	verified source-guide
[091, 2026]	SOVIET ACTIVE MEASURES AND DISINFORMATION	A declassified-in-part 1986 CIA speech text on Soviet active measures, prepared by the Foreign Activities Branch, Third World Activities Division, Office of Soviet Analysis. It explains the KGB's use of forgeries, disinformation, and front organizations to covertly influence foreign governments and publics, illustrating with the forged 1984 Olympic KKK leaflet operation designed to discourage participation in the Los Angeles Games.	verified source-guide
[092, 2026]	INTRODUCTION	A March 2019 CREST (Centre for Research and Evidence on Security Threats) report titled "Russia and Disinformation: Maskirovka," prepared by scholars of Russian foreign and security policy using open-source and Russian-language primary material. It examines the historical background of Soviet and Russian disinformation, including the concept of active measures, and how disinformation is woven into strategic narratives and diplomacy.	verified source-guide
[093, 2026]	Deception, Disinformation, and Strategic Communications	Fletcher Schoen and Christopher J. Lamb, 'Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference,' INSS Strategic Perspectives No. 11 (NDU Press, June 2012). The study examines the U.S. Active Measures Working Group, a small interagency committee formed in the 1980s to expose and counter Soviet disinformation, and analyzes why it succeeded where most such groups fail.	verified source-guide

Source	Cited work	What it contributes	Status
[094, 2026]	Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference	Fletcher Schoen and Christopher J. Lamb, 'Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference,' INSS Strategic Perspectives No. 11 (NDU Press, June 2012).	verified source-guide
[095, 2026]	COGNITIVE SECURITY IN THE AGE OF AI	This policy paper examines the emergence of cognitive security.	original source-guide
[096, 2026]	AI DEVELOPMENT SHOULD PRIORITIZE COGNITIVE SECURITY	A position paper (Stanford authors, ICLR 2026 workshop) arguing that AI research and development should prioritize cognitive security, defined as protecting human cognitive processes from hazardous influence. It notes that generative AI systems increasingly designed to influence beliefs and behavior raise acute governance concerns, while research on these effects remains fragmented.	verified source-guide
[308, 2026]	Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure	An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure.	verified source-guide
[311, 2026]	Countering Information Threats	An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering.	verified source-guide

Where this sits. This module's overview is Section 29; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

29.3.4 Active Measures and Disinformation governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 29; [238, 2026].

29.3.5 Active Measures and Disinformation analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 19's governance-boundary section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Research lane: **Cognitive Security and Influence Resilience** for **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**. [238, 2026]; [239, 2026].
Curriculum topic spine: Cognitive influence-analysis case review using sample materials, **Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**, **Declassified source-protection and institutional-control case study**. **Verified anchor cluster:** [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]; [OECD, 2026c]; [for Security Policy, 2025]; [Community, 2020a].
Conceptual depth: protecting attention, belief formation, and decision quality without turning resilience education into manipulation.
Method stack: claim decomposition, narrative provenance, inoculation framing, bias checks, audience-risk review, and after-action learning.
Composability contract: separate descriptive analysis, normative assessment, response options, and protected-audience considerations.
Known failure modes: counter-messaging as manipulation, overclaiming intent, pathologizing audiences, and collapsing uncertainty into moral certainty.
Defensive boundary: practice uses benign simulations and resilience education; it does not create persuasion campaigns, impersonation, or deception plans. Applied to **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**.

Anchor	Why it matters here
[Cybersecurity and Agency, 2024b]	Official CISA guidance on foreign influence operations targeting critical infrastructure. Checked as of 2026-05-21; role: source_quality_anchor.
[Organization, 2026b]	Official NATO counter-information-threat guidance. Checked as of 2026-05-21; role: source_quality_anchor.
[Cybersecurity and Agency, 2026b]	Official CISA election-security source for public-resilience, foreign-influence awareness, rumor control, and defensive communication framing. Checked as of 2026-05-21; role: curriculum_anchor.
[Organization, 2026c]	Official NATO source for hybrid-threat resilience across cyber, information, economic, political, and military pressure. Checked as of 2026-05-21; role: curriculum_anchor.
[OECD, 2026c]	Official OECD policy source for information integrity, governance responses, public trust, and democratic resilience. Checked as of 2026-05-21; role: curriculum_anchor.
[for Security Policy, 2025]	Policy-scholarship source for cognitive security, information literacy, critical thinking, and whole-of-society resilience. Checked as of 2026-05-21; role: curriculum_anchor.
[Community, 2020a]	Official IC framework for AI goals, authorities, human judgment, bias mitigation, testing, documentation, explainability, and review. Checked as of 2026-05-21; role: curriculum_anchor.

29.3.5.1 Active Measures and Disinformation evidence standard and citation floor: source families and discovery limits Official guidance supplies governance, safety, and legal constraints for the **Cognitive Security and Influence Resilience** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [238, 2026]; [239, 2026].

29.3.6 Active Measures and Disinformation agentic boundary: assist, approve, block, and record

Evidence anchor. Section 29; [238, 2026].
AGEINT translation is bounded by the **Cognitive Security and Influence Resilience** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**.

29.3.6.1 Active Measures and Disinformation permitted defensive utility: curriculum uses and safe outputs **Evidence anchor.** Section 29; [238, 2026].
The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**.

29.3.6.2 Active Measures and Disinformation excluded operational boundary: blocked actions and stop rules Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [238, 2026]; [239, 2026] and **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

29.3.7 Active Measures and Disinformation governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 29; [238, 2026].
Governance is practiced as a gate on the **Cognitive Security and Influence Resilience** lane. Learners use the **Cognitive-Resilience Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**.

29.3.7.1 Active Measures and Disinformation governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [238, 2026]; [239, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Cognitive Security and Influence Resilience** failure modes and the **Cognitive-Resilience Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

29.3.7.2 Active Measures and Disinformation evidence package handoff: appendices, records, and reuse **Evidence anchor.** Section 29; [238, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Cognitive-Resilience Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**.

29.3.7.3 Active Measures and Disinformation current-source assurance: verified anchors and local artifact fit The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**. [238, 2026]; [239, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_cisa_foreign_influence` for **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**?	Preparing for and Mitigating Foreign Influence Operations; lane `source_quality_spine`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official CISA guidance on foreign influence operations targeting critical infrastructure.
What does the module inherit from `official_nato_counter_information_threats` for **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**?	Countering Information Threats; lane `source_quality_spine`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official NATO counter-information-threat guidance.
What does the module inherit from `official_cisa_election_security_influence` for **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**?	Election Security; lane `cognitive_influence_security`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official CISA election-security source for public-resilience, foreign-influence awareness, rumor control, and defensive communication framing.
What does the module inherit from `official_nato_hybrid_threats` for **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**?	Countering Hybrid Threats; lane `cognitive_influence_security`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official NATO source for hybrid-threat resilience across cyber, information, economic, political, and military pressure.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 29; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

29.3.8 Active Measures and Disinformation assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 29; [238, 2026].

29.3.9 Active Measures and Disinformation assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 29; [238, 2026].

29.3.9.1 Active Measures and Disinformation capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation** and [238, 2026]; [239, 2026].

29.3.9.2 Active Measures and Disinformation instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation** and [238, 2026]; [239, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

29.3.9.3 Active Measures and Disinformation assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Cognitive influence-analysis case review using sample materials	Completed **narrative-risk map with provenance, uncertainty, audience harms, and response options** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Dezinformatsiya: Forgery, Front Organizations, Media Manipulation	Completed **narrative-risk map with provenance, uncertainty, audience harms, and response options** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Declassified source-protection and institutional-control case study	Completed **narrative-risk map with provenance, uncertainty, audience harms, and response options** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

29.3.10 Active Measures and Disinformation refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [238, 2026]; [239, 2026] and **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**.

29.3.10.1 Active Measures and Disinformation refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**. The local signals begin with [238, 2026]; [239, 2026].

29.3.10.2 Active Measures and Disinformation claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**, and the source spine for these checks begins with [238, 2026]; [239, 2026].

29.3.11 Active Measures and Disinformation reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [238, 2026]; [239, 2026].

Triangulation anchors. In module 19's review-checklist section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation**. [238, 2026]; [239, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

29.3.12 Active Measures and Disinformation learning-path links: module map, overview, and curriculum atlas

These links keep **Cognitive influence-analysis case review using sample materials; Dezinformatsiya: Forgery, Front Organizations, Media Manipulation** paired with the orientation atlas, the parent unit, and the previous and next modules, so a reader can trace which claims and caveats are inherited rather than re-derived here. Anchored at [238, 2026]; [239, 2026].

Section 2, Section 27, Section 28, Section 30

30 Social Engineering

30.0.1 Social Engineering figures and course links: visual evidence, source flow, and navigation

The module uses Figure 68 and Figure 64 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 27, Section 29, Section 31.
This module teaches the **Cognitive Security and Influence Resilience** lane through a bounded, source-backed coursebook chapter. [238, 2026]; [240, 2026].

30.1 Cognitive Security and Influence Resilience frame for Social Engineering: source context, topic focus, and reader task

Evidence anchor. Section 30; [238, 2026].

30.1.1 Social Engineering orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 30; [238, 2026].

30.1.2 Social Engineering conceptual primer: source context, core model, and reader task

This chapter teaches cognitive security as protection of attention, trust, memory, and decision quality without creating manipulation. The chapter uses **Cognitive-Resilience Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**.
The central distinction is to separate analysis of influence from persuasion design. Core topics include **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering; Social Engineering: The Science of Human Hacking (Hadnagy, 2018)**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [238, 2026]; [240, 2026].
Learners move from vocabulary and the **Cognitive-Resilience Lens** distinction through topic lessons on **The Psychology of Influence: Cialdini's Seven Principles** with evidence and misconception checks, then assemble a **narrative-risk map with provenance, uncertainty, audience harms, and response options** with safety and rights gates.

30.1.3 Social Engineering learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 30; [238, 2026].

- Connect **The Psychology of Influence: Cialdini's Seven Principles and History of Social Engineering** to **Cognitive Security and Influence Resilience** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate analysis of influence from persuasion design; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as counter-messaging as manipulation, overclaiming intent, pathologizing audiences, and collapsing uncertainty into moral certainty, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: practice uses benign simulations and resilience education; it does not create persuasion campaigns, impersonation, or deception plans.

30.1.4 Social Engineering core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 30; [238, 2026].

Term	Working definition
Narrative provenance	where a claim, frame, or story came from and how it spread
Prebunking	transparent education that helps people recognize misleading patterns before exposure
Audience harm	a privacy, dignity, autonomy, or trust risk for people receiving information
Attribution caution	the rule that intent and origin claims need strong evidence
Resilience response	a transparent education, correction, or process improvement that avoids manipulation
MISO boundary	the line between accountable public messaging analysis and covert influence design
Inoculation	building recognition of manipulation tactics without deploying persuasion against a population
The Psychology of Influence: Cialdini's Seven…	Key terms: Psychology, Influence, Cialdini.
History of Social Engineering	Key terms: History, Social, Engineering.

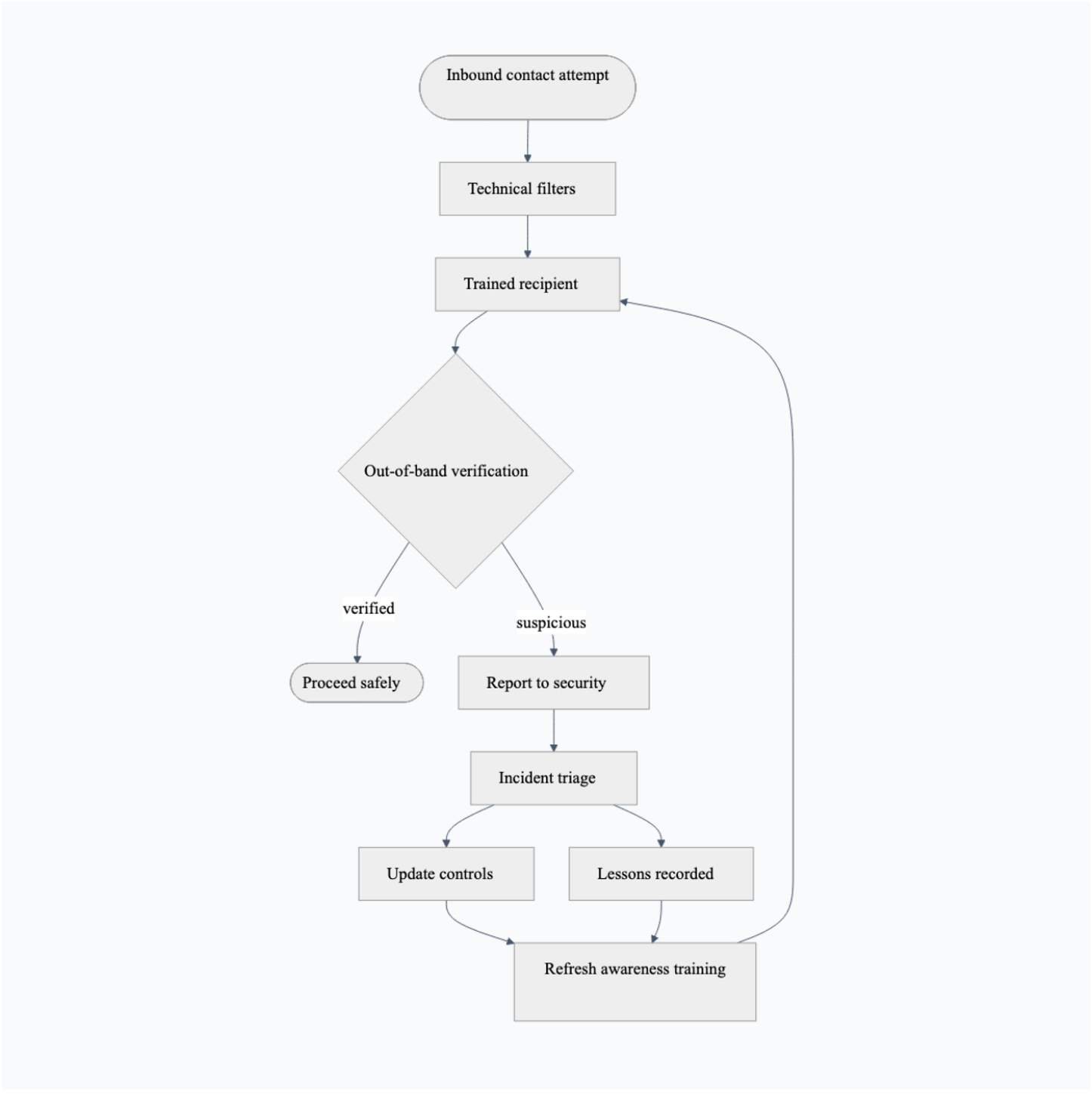


Figure 68: The layered human and technical control loop that lets an organization absorb a social-engineering attempt and convert it into a reported, learned-from event. The captioned view belongs to the psychological operations and influence / social engineering section and should be read as a map of Inbound contact attempt, Technical filters, Trained recipient, and Proceed safely, not as a capability score or live-task instruction.

30.2 Cognitive-Resilience Lens path for Social Engineering: lesson cluster, safe artifact, and review

Evidence anchor. Section 30; [238, 2026].

30.2.1 Social Engineering practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 30; [238, 2026].

30.2.2 Social Engineering topic lessons: source-backed concepts and transfer tasks

This module builds cognitive security as protection of attention, trust, memory, and decision quality without creating manipulation. The sequence opens with **The Psychology of Influence: Cialdini's Seven Principles**, **History of Social Engineering**, **Social Engineering: The Science of Human Hacking (Hadnagy, 2018)** and applies the **Cognitive-Resilience Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 64; module overview Section 30; curriculum atlas Section 2.

Triangulation anchors. In module 20's topic-lessons section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

30.2.2.1 Lesson 1: The Psychology of Influence: Cialdini's Seven Principles

Concept. The Psychology of Influence: Cialdini's Seven Principles focuses on transparent resilience education: provenance, audience harm, attribution caution, and non-manipulative response options.

Why it matters. Analysts use **The Psychology of Influence** to separate analysis of influence from persuasion design. A defensible treatment names the judgment it enables for information-integrity analysis and resilience education review, the proof limit that treating resilience labels as permission to skip provenance review would otherwise hide, and the reviewer accountable for challenge.

Source support. The Psychology of Influence: Cialdini's Seven Principles rests on [097, 2026]. The most specific cited work observes: It surveys major attack categories including phishing and its variants, pretexting, baiting, tailgating, and quid pro quo schemes, and explains the psychological influence principles such as reciprocity, scarcity, authority, and consensus that attackers exploit. Use it for fixing what **The Psychology of Influence: Cialdini's Seven Principles** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **The Psychology of Influence**, reason from the sources cited in this row. [097, 2026] This Mitnick Security guide traces the history and evolution of social engineering from antiquity through modern cyberattacks. It surveys major attack categories including phishing and its variants, pretexting, baiting, tailgating, and quid pro quo schemes, and explains the psychological influence principles such as reciprocity, scarcity, authority, and consensus that attackers exploit. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **The Psychology of Influence**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Psychology of Influence**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **The Psychology of Influence** work as a **narrative-risk and resilience map** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **The Psychology of Influence**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **The Psychology of Influence** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

30.2.2.2 Lesson 2: History of Social Engineering

Concept. History of Social Engineering teaches defensive recognition of manipulation attempts using sample messages, consent boundaries, and reporting duties.

Why it matters. History of Social Engineering matters in the **Cognitive Security and Influence Resilience** lane because information-integrity analysis and resilience education evidence must stay separate from judgment; treating resilience labels as permission to skip provenance review is a common failure.

Source support. History of Social Engineering rests on [097, 2026]. The most specific cited work observes: It surveys major attack categories including phishing and its variants, pretexting, baiting, tailgating, and quid pro quo schemes, and explains the psychological influence principles such as reciprocity, scarcity, authority, and consensus that attackers exploit. Use it for fixing what **History of Social Engineering** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Read **History of Social Engineering** against the works cited for this row. [097, 2026] This Mitnick Security guide traces the history and evolution of social engineering from antiquity through modern cyberattacks. It surveys major attack categories including phishing and its variants, pretexting, baiting, tailgating, and quid pro quo schemes, and explains the psychological influence principles such as reciprocity, scarcity, authority, and consensus that attackers exploit. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. Build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **History of Social Engineering**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape this subject work as a **narrative-risk and resilience map** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **History of Social Engineering**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Transfer **History of Social Engineering** from this module to a second motif by preserving information-integrity analysis and resilience education, replacing action with audit, and naming the blocked use.

30.2.2.3 Lesson 3: Social Engineering: The Science of Human Hacking (Hadnagy, 2018)

Concept. Social Engineering: The Science of Human Hacking (Hadnagy, 2018) teaches defensive recognition of manipulation attempts using sample messages, consent boundaries, and reporting duties.

Why it matters. Analysts use **Social Engineering: The Science of Human Hacking (Hadnagy, 2018)** to separate analysis of influence from persuasion design. A defensible treatment names the judgment it enables for information-integrity analysis and resilience education review, the proof limit that treating resilience labels as permission to skip provenance review would otherwise hide, and the reviewer accountable for challenge.

Source support. Social Engineering: The Science of Human Hacking (Hadnagy, 2018) rests on [098, 2026]. The closest source to this row notes: It is written as a professional reference on understanding and countering human-targeted security threats. Use it for the working definition that **Social Engineering: The Science of Human Hacking (Hadnagy, 2018)** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Ground **Social Engineering: The Science of Human Hacking (Hadnagy, 2018)** in the evidence the row cites. [098, 2026] The full text of "the module: The Science of Human Hacking" (2nd edition, 2018) by Christopher Hadnagy, published by John Wiley & Sons.

The book examines the human element of security, analyzing how manipulation and persuasion techniques can be used to influence people, and how individuals and organizations can recognize and defend against such tactics. It is written as a professional reference on understanding and countering human-targeted security threats. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For the module, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about the module, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Social Engineering: The Science of Human Hacking (Hadnagy, 2018)** work as a **narrative-risk and resilience map** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Social Engineering: The Science of Human Hacking (Hadnagy, 2018)**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Transfer **Social Engineering: The Science of Human Hacking (Hadnagy, 2018)** from this module to a second motif by preserving information-integrity analysis and resilience education, replacing action with audit, and naming the blocked use.

30.2.2.4 Lesson 4: The Art of Human Hacking (Hadnagy, 2010)

Concept. The Art of Human Hacking (Hadnagy, 2010) focuses on transparent resilience education: provenance, audience harm, attribution caution, and non-manipulative response options.

Why it matters. Without explicit treatment of **The Art of Human Hacking (Hadnagy, 2010)**, treating resilience labels as permission to skip provenance review undermines information-integrity analysis and resilience education review; the lesson builds the habit to separate analysis of influence from persuasion design.

Source support. The Art of Human Hacking (Hadnagy, 2010) rests on [099, 2026]. Its anchor reference records: A PDF of the book the module: The Art of Human Hacking by Christopher Hadnagy, a foundational security text on how attackers exploit human psychology rather than technical flaws to obtain information or access. Use it for fixing what **The Art of Human Hacking (Hadnagy, 2010)** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Read **The Art of Human Hacking (Hadnagy, 2010)** against the works cited for this row. [099, 2026] A PDF of the book the module: The Art of Human Hacking by Christopher Hadnagy, a foundational security text on how attackers exploit human psychology rather than technical flaws to obtain information or access. The work surveys manipulation tactics and the human factors that make organizations vulnerable, and frames this knowledge defensively to help security professionals recognize and resist such attacks. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **The Art of Human Hacking (Hadnagy, 2010)**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Art of Human Hacking**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape this subject work as a **narrative-risk and resilience map** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **The Art of Human Hacking (Hadnagy, 2010)**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Apply this module's safe boundary for **The Art of Human Hacking (Hadnagy, 2010)** to another artifact while keeping information-integrity analysis and resilience education and reviewer ownership explicit.

30.2.2.5 Lesson 5: Phishing, Vishing, Smishing, Deepfake Voice Attacks

Concept. Phishing, Vishing, Smishing, Deepfake Voice Attacks teaches defensive recognition of manipulation attempts using sample messages, consent boundaries, and reporting duties.

Why it matters. Phishing, Vishing, Smishing, Deepfake Voice Attacks connects classroom vocabulary to Cognitive Security and Influence Resilience practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Phishing, Vishing, Smishing, Deepfake Voice Attacks rests on [300, 2026], [304, 2026], and [306, 2026]. Its anchor reference records: NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Use them for fixing what **Phishing, Vishing, Smishing, Deepfake Voice Attacks** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Ground **Phishing, Vishing, Smishing, Deepfake Voice Attacks** in the evidence the row cites. [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Phishing, Vishing, Smishing, Deepfake Voice Attacks**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Phishing Vishing Smishing Deepfake Voice**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape this subject work as a **narrative-risk and resilience map** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Phishing, Vishing, Smishing, Deepfake Voice Attacks**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **Phishing, Vishing, Smishing, Deepfake Voice Attacks** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

30.2.2.6 Lesson 6: Physical Social Engineering: Access, Elicitation, Impersonation

Concept. Physical Social Engineering: Access, Elicitation, Impersonation teaches defensive recognition of manipulation attempts using sample messages, consent boundaries, and reporting duties.

Why it matters. Without explicit treatment of **Physical Social Engineering**, treating resilience labels as permission to skip provenance review undermines information-integrity analysis and resilience education review; the lesson builds the habit to separate analysis of influence from persuasion design.

Source support. Physical Social Engineering: Access, Elicitation, Impersonation rests on [308, 2026] and [311, 2026]. The closest source to this row notes: An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. Use them for the working definition that **Physical Social Engineering: Access, Elicitation, Impersonation** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Physical Social Engineering**, work from the cited evidence behind this row. [308, 2026] An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure. [311, 2026] An official NATO topic page describing the Alliance's approach to countering

information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Physical Social Engineering**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Physical Social Engineering**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Physical Social Engineering** work as a **narrative-risk and resilience map** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Physical Social Engineering**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **Physical Social Engineering** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

30.2.2.7 Lesson 7: AI Automation of Social Engineering at Scale

Concept. AI Automation of Social Engineering at Scale compares resolution, accuracy, and temporal fitness before drawing a geospatial conclusion from imagery or map products.

Why it matters. AI Automation of Social Engineering at Scale connects classroom vocabulary to Cognitive Security and Influence Resilience practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. AI Automation of Social Engineering at Scale rests on [100, 2026]. Its anchor reference records: The authors document eight attack categories and map them across static infrastructure, mobile networks, and infrastructure-free systems such as blockchain and the metaverse. Use it for the claim that **AI Automation of Social Engineering at Scale** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Read **AI Automation of Social Engineering at Scale** against the works cited for this row. [100, 2026] This survey examines how large language model-based agents can be weaponized as autonomous cyberattack tools, analyzing their architecture across five core components: models, perception, memory, reasoning and planning, and tools. The authors document eight attack categories and map them across static infrastructure, mobile networks, and infrastructure-free systems such as blockchain and the metaverse. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **AI Automation**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **AI Automation of Social Engineering**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **AI Automation of Social Engineering at Scale** work as a **narrative-risk and resilience map** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **AI Automation of Social Engineering at Scale**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **AI Automation of Social Engineering at Scale** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

30.2.2.8 Lesson 8: Defense: Training, Simulation, Technical Controls

Concept. Defense: Training, Simulation, Technical Controls focuses on transparent resilience education: provenance, audience harm, attribution caution, and non-manipulative response options.

Why it matters. Defense: Training, Simulation, Technical Controls matters in the **Cognitive Security and Influence Resilience** lane because information-integrity analysis and resilience education evidence must stay separate from judgment; treating resilience labels as permission to skip provenance review is a common failure.

Source support. Defense: Training, Simulation, Technical Controls rests on [308, 2026] and [311, 2026]. The most specific cited work observes: It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering. Use them for fixing what **Defense: Training, Simulation, Technical Controls** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Ground **Defense: Training, Simulation, Technical Controls** in the evidence the row cites. [308, 2026] An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure. [311, 2026] An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Defense**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Defense**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Defense: Training, Simulation, Technical Controls** work as a **narrative-risk and resilience map** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Defense: Training, Simulation, Technical Controls**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **Defense: Training, Simulation, Technical Controls** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

30.2.3 Social Engineering worked safe example: synthetic inputs, evidence, and review

Worked example: a sample public-library class evaluates a synthetic rumor about a community service and compares transparent correction options. [238, 2026]; [240, 2026].

Triangulation anchors. In module 20's worked-example section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **information-integrity and influence analysis**. Learners use a **narrative-risk and resilience map** and keep this boundary visible: No covert persuasion, microtargeting, manipulation, or campaign design.

Frame. The classroom question centers on **The Psychology of Influence: Cialdini's Seven Principles**. Excluded actions stay explicit, and the **Cognitive-Resilience Lens** planning question is: How does the module protect autonomy, attention, trust, and decision quality without designing persuasion?

Inputs. For the **The Psychology of Influence: Cialdini's Seven Principles** scenario, use sample posts, source timestamps, public-service facts, and a media-literacy rubric. The Cognitive-Resilience Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **The Psychology of Influence: Cialdini's Seven Principles**, students trace narrative provenance, separate observation from attribution, name audience harms, and design a transparent lesson. Pause whenever an inference about The Psychology of Influence: Cialdini's Seven Principles appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **The Psychology of Influence: Cialdini's Seven Principles** classroom scenario; unit artifact = narrative-risk and resilience map; evidence = allowed inputs; method = information-integrity analysis and resilience education; output = a narrative-risk map with caveats, response options, and no microtargeted persuasion; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **The Psychology of Influence: Cialdini's Seven Principles** as "Cognitive-Resilience Lens confirms it" is not enough. The revision ties the claim to information-integrity analysis and resilience education, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **The Psychology of Influence: Cialdini's Seven Principles** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

30.2.4 Social Engineering practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Cognitive-Resilience Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**.

Triangulation anchors. In module 20's practice-sequence section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare The Psychology of Influence: Cialdini's Seven Principles, History of Social Engineering, Social Engineering: The Science of Human Hacking; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Cognitive Security and Influence Resilience** lane.
2. Frame	Answer the lens question: How does the module protect autonomy, attention, trust, and decision quality without designing persuasion?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for The Psychology of Influence: Cialdini's Seven Principles: narrative-risk map with provenance, uncertainty, audience harms, and response options.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the narrative-risk and resilience map fields for The Psychology of Influence: Cialdini's Seven Principles.	Unit profile note.	Evidence artifacts include narrative provenance chain, audience-harm note.
4. Challenge	Test the misconception that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.	Failure-mode note.	The artifact applies the key distinction: separate analysis of influence from persuasion design.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

30.2.4.1 Social Engineering instructor notes: source reasoning, review points, and studio focus

Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**. [238, 2026]; [240, 2026].

30.2.4.2 Social Engineering extension exercise: peer validation and refresh trigger review

Evidence anchor. Section 30; [238, 2026]. Have learners swap artifacts and apply the **Cognitive-Resilience Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**.

30.2.5 Social Engineering knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 30; [238, 2026].

1. Explain how **The Psychology of Influence: Cialdini's Seven Principles** is defined here; name the source descriptor that supports the definition.
2. Contrast **The Psychology of Influence: Cialdini's Seven Principles** with **History of Social Engineering** using the **Cognitive-Resilience Lens** artifact fields.
3. Identify one failure mode from the **Cognitive Security and Influence Resilience** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which response informs people without crossing into MISO-style manipulation or unverified attribution?
5. Correct this misconception: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

30.2.5.1 Social Engineering answer quality rubric: source evidence, uncertainty, and safe transfer

Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **The Psychology of Influence: Cialdini's Seven Principles** without source evidence, uncertainty, or a safe transfer task.

30.3 Social Engineering assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 30; [238, 2026].

30.3.1 Social Engineering evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 30; [238, 2026].

30.3.2 Social Engineering transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 30; [238, 2026].

30.3.2.1 Social Engineering lineage and source tradition: profile, concepts, and first anchors This sits in the **Cognitive Security and Influence Resilience** lineage: protecting attention, belief formation, and decision quality without turning resilience education into manipulation. [238, 2026]; [240, 2026].

30.3.2.2 Social Engineering working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 30; [238, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**, with provenance and reviewability throughout.

30.3.2.3 Social Engineering knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [238, 2026]; [240, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

30.3.2.4 Social Engineering transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 30; [238, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**.
- **Evidence contract:** keep the **Cognitive Security and Influence Resilience** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

30.3.2.5 Social Engineering profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 30; [238, 2026].

The matched profile emphasizes protecting attention, belief formation, and decision quality without turning resilience education into manipulation. The method stack is claim decomposition, narrative provenance, inoculation framing, bias checks, audience-risk review, and after-action learning; the local topic cluster is **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**.

30.3.3 Social Engineering evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 30; [238, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Cognitive Security and Influence Resilience** profile tells reviewers what evidence is strong enough for the module artifact built around **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**.

30.3.3.1 Social Engineering guide source spine: inherited keys and local citation roles Primary guide citations: [238, 2026]; [240, 2026]; [242, 2026]; [280, 2026]; [281, 2026]; [282, 2026]; [292, 2026]; [295, 2026]; [296, 2026]; [097, 2026]; [098, 2026]; [099, 2026]; [100, 2026]; [300, 2026]; [304, 2026]; [306, 2026]; [308, 2026]; [311, 2026].

30.3.3.2 Social Engineering verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [238, 2026]; [240, 2026].

Tier	What counts	How it is used
Source guide	[238, 2026]; [240, 2026]; [242, 2026]; [280, 2026]; [281, 2026]; [282, 2026]; [292, 2026]; [295, 2026]; [296, 2026]; [097, 2026]; [098, 2026]; [099, 2026]; [100, 2026]; [300, 2026]; [304, 2026]; [306, 2026]; [308, 2026]; [311, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 20's source-canon section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering** and [238, 2026]; [240, 2026], but only directly verified source URLs are encoded as citations.

30.3.3.3 Social Engineering intelligence practice lens: evidence artifact and safety check Practice lens: **Cognitive-Resilience Lens** for **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**. [238, 2026]; [240, 2026].

Planning question: How does the module protect autonomy, attention, trust, and decision quality without designing persuasion?

Evidence artifact: narrative-risk map with provenance, uncertainty, audience harms, and response options.

Validation rule: distinguish observation, attribution, impact assessment, and resilience response. Applied to **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**.

Handoff contract: handoff supports transparency, education, and resilience, not microtargeted influence or deception.

Safety check: exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning.

30.3.3.4 Social Engineering runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 30; [238, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	20.99	20.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Social Engineering to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Bounded autonomy, procurement, incident-response, and assurance studio	20.101	20.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Social Engineering	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Model-card, recoverability, retention, and learner-support evidence package	20.102	20.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Social Engineering	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
The Psychology of Influence: Cialdini's Seven Principles	20.1	20.1 The Psychology of Influence: Cialdini's Seven Principles	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
History of Social Engineering	20.2	20.2 History of Social Engineering	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Social Engineering: The Science of Human Hacking (Hadnagy, 2018)	20.3	20.3 Social Engineering: The Science of Human Hacking (Hadnagy, 2018)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
The Art of Human Hacking (Hadnagy, 2010)	20.4	20.4 The Art of Human Hacking (Hadnagy, 2010)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Phishing, Vishing, Smishing, Deepfake Voice Attacks	20.5	20.5 Phishing, Vishing, Smishing, Deepfake Voice Attacks	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Physical Social Engineering: Access, Elicitation, Impersonation	20.6	20.6 Physical Social Engineering: Access, Elicitation, Impersonation	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
AI Automation of Social Engineering at Scale	20.7	20.7 AI Automation of Social Engineering at Scale	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Defense: Training, Simulation, Technical Controls	20.8	20.8 Defense: Training, Simulation, Technical Controls	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning

30.3.3.5 Social Engineering reusable subsection contract: topic rows, artifacts, and safety duties **Evidence anchor.** Section 30; [238, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
The Psychology of Influence: Cialdini's Seven Principles	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
History of Social Engineering	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Social Engineering: The Science of Human Hacking (Hadnagy, 2018)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
The Art of Human Hacking (Hadnagy, 2010)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Phishing, Vishing, Smishing, Deepfake Voice Attacks	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Physical Social Engineering: Access, Elicitation, Impersonation	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
AI Automation of Social Engineering at Scale	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Defense: Training, Simulation, Technical Controls	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning

30.3.3.6 Social Engineering annotated source ledger: real titles and local contribution Each source cited by this **Cognitive Security and Influence Resilience** module is paired below with its real title and a one-line note on what it contributes to **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**.

Source	Cited work	What it contributes	Status
[238, 2026]	Recommendation on the Ethics of Artificial Intelligence	The official UNESCO page for the Recommendation on the Ethics of Artificial Intelligence, the first global standard-setting instrument on AI ethics, adopted in 2021 and applicable to all 194 member states. It outlines four core values, including human rights protection and environmental flourishing, and ten guiding principles such as proportionality, privacy, transparency, and fairness.	verified source-guide
[240, 2026]	The Right to Privacy in the Digital Age	The Office of the High Commissioner for Human Rights (OHCHR) hub page on the right to privacy in the digital age. It addresses how data-intensive technologies, particularly artificial intelligence, create risks for privacy, autonomy, and human dignity, and curates international standards, reports, and expert consultations.	verified source-guide
[242, 2026]	Guidance for Generative AI in Education and Research	Official UNESCO generative AI education guidance.	original source-guide
[280, 2026]	NIST SP 800-61 Rev. 3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management	NIST SP 800-61 Rev. 3, published April 2025, integrates incident response guidance into broader cybersecurity risk management aligned with the NIST Cybersecurity Framework 2.0, superseding the 2012 Rev. 2. The publication addresses cyber threat information sharing, incident handling and management practices, and procedures for detecting, responding to, and recovering from security incidents.	verified source-guide
[281, 2026]	Artificial Intelligence Cybersecurity Challenges	An ENISA (European Union Agency for Cybersecurity) report published December 15, 2020 mapping the cybersecurity challenges of artificial intelligence. It defines AI scope through a lifecycle approach, identifies the assets requiring protection within AI ecosystems, and develops a threat taxonomy classified across lifecycle stages and asset categories.	verified source-guide
[282, 2026]	AI Research: Security and Resilience	A NIST page on AI research focused on security and resilience, framing these as core characteristics of trustworthy AI under the NIST AI Risk Management Framework.	verified source-guide
[292, 2026]	Assessing Risks and Impacts of AI (ARIA): Pilot Evaluation Report	The ARIA 0.1 pilot evaluation report documents NIST's methodology for systematically assessing AI applications for risks and societal impacts, using a multi-layered evaluation approach across five participating organizations and seven submitted AI applications. The pilot employed three evaluation scenarios and three testing levels: model testing, red teaming, and field testing, supplemented by dialogue annotation, tester questionnaires, and structured measurement trees.	verified source-guide

Source	Cited work	What it contributes	Status
[295, 2026]	M-25-22: Driving Efficient Acquisition of Artificial Intelligence in Government	OMB Memorandum M-25-22 (April 3, 2025), Driving Efficient Acquisition of Artificial Intelligence in Government, issued under Executive Order 13960 and related directives. It provides guidance to federal agencies for acquiring effective and trustworthy AI in a timely, cost-effective manner, and rescinds and replaces earlier memorandum M-24-18.	verified source-guide
[296, 2026]	Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile	NIST AI 600-1, the Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, a cross-sectoral companion resource to the NIST AI RMF 1.0 issued pursuant to Executive Order 14110. It identifies risks that are unique to or amplified by generative AI and organizes suggested actions for managing those risks, mapped to the AI RMF functions.	verified source-guide
[097, 2026]	The History of Social Engineering	This Mitnick Security guide traces the history and evolution of social engineering from antiquity through modern cyberattacks. It surveys major attack categories including phishing and its variants, pretexting, baiting, tailgating, and quid pro quo schemes, and explains the psychological influence principles such as reciprocity, scarcity, authority, and consensus that attackers exploit.	verified source-guide
[098, 2026]	Social Engineering: T he Science of Human Hacking	The full text of "Social Engineering: The Science of Human Hacking" (2nd edition, 2018) by Christopher Hadnagy, published by John Wiley & Sons. The book examines the human element of security, analyzing how manipulation and persuasion techniques can be used to influence people, and how individuals and organizations can recognize and defend against such tactics. It is written as a professional reference on understanding and countering human-targeted security threats.	verified source-guide
[099, 2026]	Social Engineering: The Art of Human Hacking	A PDF of the book Social Engineering: The Art of Human Hacking by Christopher Hadnagy, a foundational security text on how attackers exploit human psychology rather than technical flaws to obtain information or access. The work surveys manipulation tactics and the human factors that make organizations vulnerable, and frames this knowledge defensively to help security professionals recognize and resist such attacks.	verified source-guide
[100, 2026]	A Survey on Large Language Model-based Agents in Autonomous	This survey examines how large language model-based agents can be weaponized as autonomous cyberattack tools, analyzing their architecture across five core components: models, perception, memory, reasoning and planning, and tools. The authors document eight attack categories and map them across static infrastructure, mobile networks, and infrastructure-free systems such as blockchain and the metaverse.	verified source-guide

Source	Cited work	What it contributes	Status
[300, 2026]	MITRE ATLAS	MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy.	original source-guide
[304, 2026]	Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities	NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences.	verified source-guide
[306, 2026]	Artificial Intelligence	Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support.	original source-guide
[308, 2026]	Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure	An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure.	verified source-guide
[311, 2026]	Countering Information Threats	An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering.	verified source-guide

Where this sits. This module's overview is Section 30; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

30.3.4 Social Engineering governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 30; [238, 2026].

30.3.5 Social Engineering analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 20's governance-boundary section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Research lane: **Cognitive Security and Influence Resilience** for **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**. [238, 2026]; [240, 2026].
Curriculum topic spine: The Psychology of Influence: Cialdini's Seven Principles, **History of Social Engineering**, **Social Engineering: The Science of Human Hacking (Hadnagy, 2018)**. **Verified anchor cluster:** [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]; [OECD, 2026c]; [for Security Policy, 2025]; [Community, 2020a].
Conceptual depth: protecting attention, belief formation, and decision quality without turning resilience education into manipulation.
Method stack: claim decomposition, narrative provenance, inoculation framing, bias checks, audience-risk review, and after-action learning.
Composability contract: separate descriptive analysis, normative assessment, response options, and protected-audience considerations.
Known failure modes: counter-messaging as manipulation, overclaiming intent, pathologizing audiences, and collapsing uncertainty into moral certainty.
Defensive boundary: practice uses benign simulations and resilience education; it does not create persuasion campaigns, impersonation, or deception plans. Applied to **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**.

Anchor	Why it matters here
[Cybersecurity and Agency, 2024b]	Official CISA guidance on foreign influence operations targeting critical infrastructure. Checked as of 2026-05-21; role: source_quality_anchor.
[Organization, 2026b]	Official NATO counter-information-threat guidance. Checked as of 2026-05-21; role: source_quality_anchor.
[Cybersecurity and Agency, 2026b]	Official CISA election-security source for public-resilience, foreign-influence awareness, rumor control, and defensive communication framing. Checked as of 2026-05-21; role: curriculum_anchor.
[Organization, 2026c]	Official NATO source for hybrid-threat resilience across cyber, information, economic, political, and military pressure. Checked as of 2026-05-21; role: curriculum_anchor.
[OECD, 2026c]	Official OECD policy source for information integrity, governance responses, public trust, and democratic resilience. Checked as of 2026-05-21; role: curriculum_anchor.
[for Security Policy, 2025]	Policy-scholarship source for cognitive security, information literacy, critical thinking, and whole-of-society resilience. Checked as of 2026-05-21; role: curriculum_anchor.
[Community, 2020a]	Official IC framework for AI goals, authorities, human judgment, bias mitigation, testing, documentation, explainability, and review. Checked as of 2026-05-21; role: curriculum_anchor.

30.3.5.1 Social Engineering evidence standard and citation floor: source families and discovery limits Official guidance supplies governance, safety, and legal constraints for the **Cognitive Security and Influence Resilience** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [238, 2026]; [240, 2026].

30.3.6 Social Engineering agentic boundary: assist, approve, block, and record

Evidence anchor. Section 30; [238, 2026].
AGEINT translation is bounded by the **Cognitive Security and Influence Resilience** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**.

30.3.6.1 Social Engineering permitted defensive utility: curriculum uses and safe outputs **Evidence anchor.** Section 30; [238, 2026].
The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**.

30.3.6.2 Social Engineering excluded operational boundary: blocked actions and stop rules Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [238, 2026]; [240, 2026] and **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

30.3.7 Social Engineering governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 30; [238, 2026].
Governance is practiced as a gate on the **Cognitive Security and Influence Resilience** lane. Learners use the **Cognitive-Resilience Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**.

30.3.7.1 Social Engineering governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials

Gate	Coursebook check	Evidence retained
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [238, 2026]; [240, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Cognitive Security and Influence Resilience** failure modes and the **Cognitive-Resilience Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

30.3.7.2 Social Engineering evidence package handoff: appendices, records, and reuse

Evidence anchor. Section 30; [238, 2026]. Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Cognitive-Resilience Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**.

30.3.7.3 Social Engineering current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**. [238, 2026]; [240, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_cisa_foreign_influence` for **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**?	Preparing for and Mitigating Foreign Influence Operations; lane `source_quality_spine`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official CISA guidance on foreign influence operations targeting critical infrastructure.
What does the module inherit from `official_nato_counter_information_threats` for **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**?	Countering Information Threats; lane `source_quality_spine`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official NATO counter-information-threat guidance.
What does the module inherit from `official_cisa_election_security_influence` for **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**?	Election Security; lane `cognitive_influence_security`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official CISA election-security source for public-resilience, foreign-influence awareness, rumor control, and defensive communication framing.
What does the module inherit from `official_nato_hybrid_threats` for **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**?	Countering Hybrid Threats; lane `cognitive_influence_security`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official NATO source for hybrid-threat resilience across cyber, information, economic, political, and military pressure.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 30; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

30.3.8 Social Engineering assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 30; [238, 2026].

30.3.9 Social Engineering assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 30; [238, 2026].

30.3.9.1 Social Engineering capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**.
Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering** and [238, 2026]; [240, 2026].

30.3.9.2 Social Engineering instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering** and [238, 2026]; [240, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

30.3.9.3 Social Engineering assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
The Psychology of Influence: Cialdini's Seven Principles	Completed **narrative-risk map with provenance, uncertainty, audience harms, and response options** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
History of Social Engineering	Completed **narrative-risk map with provenance, uncertainty, audience harms, and response options** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Social Engineering: The Science of Human Hacking (Hadnagy, 2018)	Completed **narrative-risk map with provenance, uncertainty, audience harms, and response options** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

30.3.10 Social Engineering refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [238, 2026]; [240, 2026] and **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**.

30.3.10.1 Social Engineering refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**. The local signals begin with [238, 2026]; [240, 2026].

30.3.10.2 Social Engineering claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**, and the source spine for these checks begins with [238, 2026]; [240, 2026].

30.3.11 Social Engineering reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [238, 2026]; [240, 2026].
Triangulation anchors. In module 20's review-checklist section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering**. [238, 2026]; [240, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

30.3.12 Social Engineering learning-path links: module map, overview, and curriculum atlas

These links keep **The Psychology of Influence: Cialdini's Seven Principles; History of Social Engineering** paired with the orientation atlas, the parent unit, and the previous and next modules, so a reader can trace which claims and caveats are inherited rather than re-derived here. Anchored at [238, 2026]; [240, 2026].
Section 2, Section 27, Section 29, Section 31

31 Information Warfare and Cognitive Security

31.0.1 Information Warfare and Cognitive Security figures and course links: visual evidence, source flow, and navigation

The module uses Figure 69 and Figure 64 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 27, Section 30, Section 32.
This module teaches the **Cognitive Security and Influence Resilience** lane through a bounded, source-backed coursebook chapter. [238, 2026]; [239, 2026].

31.1 Cognitive Security and Influence Resilience frame for Information Warfare and Cognitive Security: source context, topic focus, and reader task

Evidence anchor. Section 31; [238, 2026].

31.1.1 Information Warfare and Cognitive Security orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 31; [238, 2026].

31.1.2 Information Warfare and Cognitive Security conceptual primer: source context, core model, and reader task

This chapter teaches cognitive security as protection of attention, trust, memory, and decision quality without creating manipulation. The chapter uses **Cognitive-Resilience Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**.
The central distinction is to separate analysis of influence from persuasion design. Core topics include **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness; Automated Influence and the Cognitive Security Challenge**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [238, 2026]; [239, 2026].
Learners move from vocabulary and the **Cognitive-Resilience Lens** distinction through topic lessons on **Information Warfare Doctrine: Definitions, Theory, Air Force Policy** with evidence and misconception checks, then assemble a **narrative-risk map with provenance, uncertainty, audience harms, and response options** with safety and rights gates.

31.1.3 Information Warfare and Cognitive Security learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 31; [238, 2026].

- Connect **Information Warfare Doctrine: Definitions, Theory, Air Force Policy and Military Deception: Six Principles and Historical Effectiveness** to **Cognitive Security and Influence Resilience** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate analysis of influence from persuasion design; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as counter-messaging as manipulation, overclaiming intent, pathologizing audiences, and collapsing uncertainty into moral certainty, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: practice uses benign simulations and resilience education; it does not create persuasion campaigns, impersonation, or deception plans.

31.1.4 Information Warfare and Cognitive Security core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 31; [238, 2026].

Term	Working definition
Narrative provenance	where a claim, frame, or story came from and how it spread
Prebunking	transparent education that helps people recognize misleading patterns before exposure
Audience harm	a privacy, dignity, autonomy, or trust risk for people receiving information
Attribution caution	the rule that intent and origin claims need strong evidence
Resilience response	a transparent education, correction, or process improvement that avoids manipulation
MISO boundary	the line between accountable public messaging analysis and covert influence design
Inoculation	building recognition of manipulation tactics without deploying persuasion against a population
Information Warfare Doctrine: Definitions,…	Key terms: Information, Warfare, Doctrine.
Military Deception: Six Principles and…	Key terms: Military, Deception, Six.

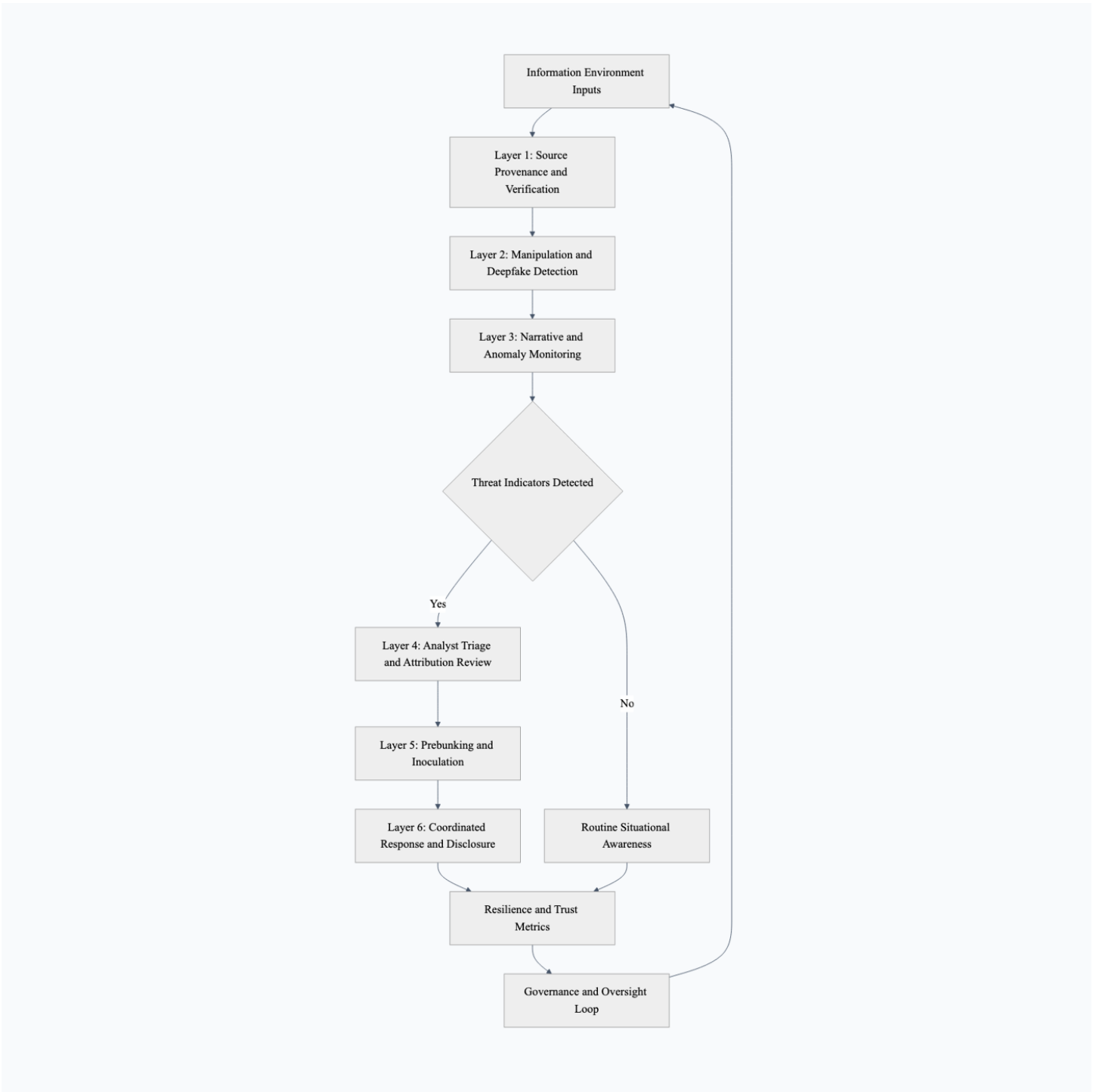


Figure 69: A layered defensive control stack for cognitive security, moving from source verification and manipulation detection through analyst triage, inoculation, and a governed response loop. It is anchored to the psychological operations and influence / information warfare and cognitive security section; use it to inspect Information Environment Inputs, Layer 1: Source Provenance and Verification, Layer 2: Manipulation and Deepfake Detection, and Layer 3: Narrative and Anomaly Monitoring while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

31.2 Cognitive-Resilience Lens path for Information Warfare and Cognitive Security: lesson cluster, safe artifact, and review

Evidence anchor. Section 31; [238, 2026].

31.2.1 Information Warfare and Cognitive Security practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 31; [238, 2026].

31.2.2 Information Warfare and Cognitive Security topic lessons: source-backed concepts and transfer tasks

This module builds cognitive security as protection of attention, trust, memory, and decision quality without creating manipulation. The sequence opens with **Information Warfare Doctrine: Definitions, Theory, Air Force Policy**, **Military Deception: Six Principles and Historical Effectiveness**, **Automated Influence and the Cognitive Security Challenge** and applies the **Cognitive-Resilience Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 64; module overview Section 31; curriculum atlas Section 2.

Triangulation anchors. In module 21's topic-lessons section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

31.2.2.1 Lesson 1: Information Warfare Doctrine: Definitions, Theory, Air Force Policy **Concept. Information Warfare Doctrine: Definitions, Theory, Air Force Policy** analyzes information warfare through narrative provenance, audience harm, and transparent resilience—not influence operations design.

Why it matters. Information Warfare Doctrine matters in the **Cognitive Security and Influence Resilience** lane because information-integrity analysis and resilience education evidence must stay separate from judgment; treating resilience labels as permission to skip provenance review is a common failure.

Source support. Information Warfare Doctrine: Definitions, Theory, Air Force Policy rests on [101, 2026] and [102, 2026]. Its anchor reference records: A 2006 paper by William Hutchinson published in the journal Informing Science. Use them for pinning down the scope of **Information Warfare Doctrine: Definitions, Theory, Air Force Policy**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Read **Information Warfare Doctrine** against the works cited for this row. [101, 2026] The military's use or misuse of information in psychological or deception operations, under. [102, 2026] A 2006 paper by William Hutchinson published in the journal Informing Science. It examines the history of information warfare and the increasingly central role of deception within it, tracing the concept from its late-1980s origins as a technology-oriented military tactic for command-and-control dominance to a broader recognition of information itself as both weapon and target. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Information Warfare Doctrine**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Information Warfare Doctrine**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Information Warfare Doctrine** work as a **narrative-risk and resilience map** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Information Warfare Doctrine**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **Information Warfare Doctrine** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

31.2.2.2 Lesson 2: Military Deception: Six Principles and Historical Effectiveness **Concept. Military Deception: Six Principles and Historical Effectiveness** compares deception indicators with alternative explanations and uncertainty before any operational inference.

Why it matters. Military Deception connects classroom vocabulary to Cognitive Security and Influence Resilience practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Military Deception: Six Principles and Historical Effectiveness rests on [103, 2026] and [104, 2026]. The lead source's own note reads: Featured pieces argue that information operations officers should be conceptualized primarily as deception officers, and one quantitative reassessment reports that deception is employed in roughly 30 to 53 percent of military operations. Use them for fixing what **Military Deception: Six Principles and Historical Effectiveness** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Ground **Military Deception** in the evidence the row cites. [103, 2026] A topic page from the Journal of Information Warfare collecting scholarly articles on military deception. Featured pieces argue that information operations officers should be conceptualized primarily as deception officers, and one quantitative reassessment reports that deception is employed in roughly 30 to 53 percent of military operations. [104, 2026] An essay published in Small Wars Journal (June 2025) by a U.S. Army Civil Affairs officer arguing that military deception and information operations have become central to modern conflict. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Military Deception**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Military Deception**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Military Deception** work as a **narrative-risk and resilience map** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Military Deception**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Transfer **Military Deception** from this module to a second motif by preserving information-integrity analysis and resilience education, replacing action with audit, and naming the blocked use.

31.2.2.3 Lesson 3: Automated Influence and the Cognitive Security Challenge **Concept. Automated Influence and the Cognitive Security Challenge** maps cognitive attack surfaces: attention, belief formation, narrative provenance, and transparent correction options.

Why it matters. Without explicit treatment of **Automated Influence**, treating resilience labels as permission to skip provenance review undermines information-integrity analysis and resilience education review; the lesson builds the habit to separate analysis of influence from persuasion design.

Source support. Automated Influence and the Cognitive Security Challenge rests on [105, 2026]. Its anchor reference records: Sarah Rajtmajer and Daniel Susser, 'Automated Influence and the Challenge of Cognitive Security,' in Hot Topics in the Science of Security (HotSoS '20), April 2020, ACM. Use it for fixing what **Automated Influence and the Cognitive Security Challenge** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Automated Influence**, reason from the sources cited in this row. [105, 2026] Sarah Rajtmajer and Daniel Susser, 'Automated Influence and the Challenge of Cognitive Security,' in Hot Topics in the Science of Security (HotSoS '20), April 2020, ACM. The paper argues that AI-powered computational propaganda poses national security threats that existing ethical frameworks do not address, and proposes 'cognitive security' as a productive conceptual lens for evaluating the ethics of automated influence operations and potential defensive responses. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Automated Influence**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Automated Influence and the Cognitive**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Automated Influence** work as a **narrative-risk and resilience map** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Automated Influence**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Apply this module's safe boundary for **Automated Influence** to another artifact while keeping information-integrity analysis and resilience education and reviewer ownership explicit.

31.2.2.4 Lesson 4: Cognitive Security in the Age of AI: NATO/EU Paradigm Shift

Concept. Cognitive Security in the Age of AI: NATO/EU Paradigm Shift maps cognitive attack surfaces: attention, belief formation, narrative provenance, and transparent correction options.

Why it matters. Analysts use **Cognitive Security in the Age of AI** to separate analysis of influence from persuasion design. A defensible treatment names the judgment it enables for information-integrity analysis and resilience education review, the proof limit that treating resilience labels as permission to skip provenance review would otherwise hide, and the reviewer accountable for challenge.

Source support. Cognitive Security in the Age of AI: NATO/EU Paradigm Shift rests on [095, 2026]. The closest source to this row notes: This policy paper examines the emergence of cognitive security. Use it for fixing what **Cognitive Security in the Age of AI: NATO/EU Paradigm Shift** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Cognitive Security in the Age of AI**, reason from the sources cited in this row. [095, 2026] This policy paper examines the emergence of cognitive security. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Cognitive Security in the Age of AI**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Cognitive Security in the Age**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Cognitive Security in the Age of AI** work as a **narrative-risk and resilience map** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Cognitive Security in the Age of AI**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **Cognitive Security in the Age of AI** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

31.2.2.5 Lesson 5: Epistemic Chaos as an Adversarial Goal

Concept. Epistemic Chaos as an Adversarial Goal protects knowledge production with provenance, dissent channels, and transparent correction—not narrative control.

Why it matters. Without explicit treatment of **Epistemic Chaos**, treating resilience labels as permission to skip provenance review undermines information-integrity analysis and resilience education review; the lesson builds the habit to separate analysis of influence from persuasion design.

Source support. Epistemic Chaos as an Adversarial Goal rests on [095, 2026] and [096, 2026]. The closest source to this row notes: It notes that generative AI systems increasingly designed to influence beliefs and behavior raise acute governance concerns, while research on these effects remains fragmented. Use them for pinning down the scope of **Epistemic Chaos as an Adversarial Goal**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Epistemic Chaos**, work from the cited evidence behind this row. [095, 2026] This policy paper examines the emergence of cognitive security. [096, 2026] A position paper (Stanford authors, ICLR 2026 workshop) arguing that AI research and development should prioritize cognitive security, defined as protecting human cognitive processes from hazardous influence. It notes that generative AI systems increasingly designed to influence beliefs and behavior raise acute governance concerns, while research on these effects remains fragmented. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Epistemic Chaos**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Epistemic Chaos as an Adversarial**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Epistemic Chaos** work as a **narrative-risk and resilience map** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Epistemic Chaos**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **Epistemic Chaos** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

31.2.2.6 Lesson 6: Active Inference and Predictive Processing as Models for Cognitive Attack/Defense

Concept. Active Inference and Predictive Processing as Models for Cognitive Attack/Defense treats the free-energy principle as computational-neuroscience theory, define prediction error, generative model, and uncertainty in plain language, then show how the theory helps an analyst notice when a model is explaining too much from too little evidence.

Why it matters. Active Inference connects classroom vocabulary to Cognitive Security and Influence Resilience practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Active Inference and Predictive Processing as Models for Cognitive Attack/Defense rests on [106, 2026] and [003, 2026]. Its anchor reference records: A 2024 bachelor's thesis by Lara Sakarya at Delft University of Technology presenting a systematic literature review of the active inference framework and the free-energy principle as applied to mimicking social human behavior in intelligent agents. Use them for pinning down the scope of **Active Inference and Predictive Processing as Models for Cognitive Attack/Defense**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Active Inference**, reason from the sources cited in this row. [106, 2026] A 2024 bachelor's thesis by Lara Sakarya at Delft University of Technology presenting a systematic literature review of the active inference framework and the free-energy principle as applied to mimicking social human behavior in intelligent agents. It explains active inference as a theory describing behavior that minimizes surprise, and surveys model variants such as deep active inference, multimodal deep belief networks, predictive coding, and probabilistic programming. [003, 2026] A 2021 peer-reviewed article by Stephen Fox in the journal Entropy that relates the active inference framework to social organization. It maps concepts such as variational free energy, prediction error, generative models, and Markov blankets onto industrial engineering and quality management practices,

treating organizational survival as the maintenance of process control limits. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Active Inference**, build a prediction-error concept card linking formal source, surprise, model assumption, analogy limit, and reviewer checkpoint. Shape **Active Inference** work as a **narrative-risk and resilience map** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Active Inference**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. For **Active Inference**, transfer the idea to a non-AI chapter by naming the assumed model, the surprising observation, and the review point before any decision follows.

31.2.2.7 Lesson 7: Behavioral Outcomes of Human Cognitive Security (arXiv 2026)

Concept. Behavioral Outcomes of Human Cognitive Security (arXiv 2026) maps cognitive attack surfaces: attention, belief formation, narrative provenance, and transparent correction options.

Why it matters. Behavioral Outcomes matters in the **Cognitive Security and Influence Resilience** lane because information-integrity analysis and resilience education evidence must stay separate from judgment; treating resilience labels as permission to skip provenance review is a common failure.

Source support. Behavioral Outcomes of Human Cognitive Security (arXiv 2026) rests on [107, 2026]. The lead source's own note reads: An arXiv research paper (March 2026) proposing an integrative modeling framework for human cognitive security, defined as the degree to which people rely on truthful information to make truth-aligned judgments. Use it for pinning down the scope of **Behavioral Outcomes of Human Cognitive Security (arXiv 2026)**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Behavioral Outcomes**, reason from the sources cited in this row. [107, 2026] An arXiv research paper (March 2026) proposing an integrative modeling framework for human cognitive security, defined as the degree to which people rely on truthful information to make truth-aligned judgments. It synthesizes Bayesian belief-updating with Prospect Theory to model how cognitive resources and emotional valuation shape behavior, and identifies three observable outcomes: veracity discernment, task-oriented actions, and information sharing. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Behavioral Outcomes**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Behavioral Outcomes of Human Cognitive**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Behavioral Outcomes** work as a **narrative-risk and resilience map** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Behavioral Outcomes**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Transfer **Behavioral Outcomes** from this module to a second motif by preserving information-integrity analysis and resilience education, replacing action with audit, and naming the blocked use.

31.2.3 Information Warfare and Cognitive Security worked safe example: synthetic inputs, evidence, and review

Worked example: a sample public-library class evaluates a synthetic rumor about a community service and compares transparent correction options. [238, 2026]; [239, 2026].

Triangulation anchors. In module 21's worked-example section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **information-integrity and influence analysis**. Learners use a **narrative-risk and resilience map** and keep this boundary visible: No covert persuasion, microtargeting, manipulation, or campaign design.

Frame. The classroom question centers on **Information Warfare Doctrine: Definitions, Theory, Air Force Policy**. Excluded actions stay explicit, and the **Cognitive-Resilience Lens** planning question is: How does the module protect autonomy, attention, trust, and decision quality without designing persuasion?

Inputs. For the **Information Warfare Doctrine: Definitions, Theory, Air Force Policy** scenario, use sample posts, source timestamps, public-service facts, and a media-literacy rubric. The Cognitive-Resilience Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Information Warfare Doctrine: Definitions, Theory, Air Force Policy**, students trace narrative provenance, separate observation from attribution, name audience harms, and design a transparent lesson. Pause whenever an inference about Information Warfare Doctrine: Definitions, Theory, Air Force Policy appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Information Warfare Doctrine: Definitions, Theory, Air Force Policy** classroom scenario; unit artifact = narrative-risk and resilience map; evidence = allowed inputs; method = information-integrity analysis and resilience education; output = a narrative-risk map with caveats, response options, and no microtargeted persuasion; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Information Warfare Doctrine: Definitions, Theory, Air Force Policy** as "Cognitive-Resilience Lens confirms it" is not enough. The revision ties the claim to information-integrity analysis and resilience education, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Information Warfare Doctrine: Definitions, Theory, Air Force Policy** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

31.2.4 Information Warfare and Cognitive Security practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Cognitive-Resilience Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**.

Triangulation anchors. In module 21's practice-sequence section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Information Warfare Doctrine: Definitions, Theory, Air Force Policy, Military Deception: Six Principles and Historical Effectiveness, Automated Influence and the Cognitive Security Challenge; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Cognitive Security and Influence Resilience** lane.
2. Frame	Answer the lens question: How does the module protect autonomy, attention, trust, and decision quality without designing persuasion?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Information Warfare Doctrine: Definitions, Theory, Air Force Policy: narrative-risk map with provenance, uncertainty, audience harms, and response options.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the narrative-risk and resilience map fields for Information Warfare Doctrine: Definitions, Theory, Air Force Policy.	Unit profile note.	Evidence artifacts include narrative provenance chain, audience-harm note.
4. Challenge	Test the misconception that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.	Failure-mode note.	The artifact applies the key distinction: separate analysis of influence from persuasion design.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

31.2.4.1 Information Warfare and Cognitive Security instructor notes: source reasoning, review points, and studio focus Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**. [238, 2026]; [239, 2026].

31.2.4.2 Information Warfare and Cognitive Security extension exercise: peer validation and refresh trigger review Evidence anchor. Section 31; [238, 2026].

Have learners swap artifacts and apply the **Cognitive-Resilience Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**.

31.2.5 Information Warfare and Cognitive Security knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 31; [238, 2026].

1. Explain how **Information Warfare Doctrine: Definitions, Theory, Air Force Policy** is defined here; name the source descriptor that supports the definition.
2. Contrast **Information Warfare Doctrine: Definitions, Theory, Air Force Policy** with **Military Deception: Six Principles and Historical Effectiveness** using the **Cognitive-Resilience Lens** artifact fields.
3. Identify one failure mode from the **Cognitive Security and Influence Resilience** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which response informs people without crossing into MISO-style manipulation or unverified attribution?
5. Correct this misconception: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

31.2.5.1 Information Warfare and Cognitive Security answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Information Warfare Doctrine: Definitions, Theory, Air Force Policy** without source evidence, uncertainty, or a safe transfer task.

31.3 Information Warfare and Cognitive Security assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 31; [238, 2026].

31.3.1 Information Warfare and Cognitive Security evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 31; [238, 2026].

31.3.2 Information Warfare and Cognitive Security transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 31; [238, 2026].

31.3.2.1 Information Warfare and Cognitive Security lineage and source tradition: profile, concepts, and first anchors This sits in the **Cognitive Security and Influence Resilience** lineage: protecting attention, belief formation, and decision quality without turning resilience education into manipulation. [238, 2026]; [239, 2026].

31.3.2.2 Information Warfare and Cognitive Security working model: inputs, constraints, transforms, outputs, and oversight Evidence anchor. Section 31; [238, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**, with provenance and reviewability throughout.

31.3.2.3 Information Warfare and Cognitive Security knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [238, 2026]; [239, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

31.3.2.4 Information Warfare and Cognitive Security transfer contracts: authority, evidence, tools, and auditable output Evidence anchor. Section 31; [238, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**.
- **Evidence contract:** keep the **Cognitive Security and Influence Resilience** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

31.3.2.5 Information Warfare and Cognitive Security profile emphasis and local focus: method stack and topic cluster Evidence anchor. Section 31; [238, 2026].

The matched profile emphasizes protecting attention, belief formation, and decision quality without turning resilience education into manipulation. The method stack is claim decomposition, narrative provenance, inoculation framing, bias checks, audience-risk review, and after-action learning; the local topic cluster is **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**.

31.3.3 Information Warfare and Cognitive Security evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 31; [238, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Cognitive Security and Influence Resilience** profile tells reviewers what evidence is strong enough for the module artifact built around **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**.

31.3.3.1 Information Warfare and Cognitive Security guide source spine: inherited keys and local citation roles Primary guide citations: [238, 2026]; [239, 2026]; [244, 2026]; [273, 2026]; [276, 2026]; [285, 2026]; [286, 2026]; [290, 2026]; [294, 2026]; [101, 2026]; [102, 2026]; [103, 2026]; [104, 2026]; [105, 2026]; [095, 2026]; [096, 2026]; [106, 2026]; [003, 2026]; [107, 2026].

31.3.3.2 Information Warfare and Cognitive Security verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [238, 2026]; [239, 2026].

Tier	What counts	How it is used
Source guide	[238, 2026]; [239, 2026]; [244, 2026]; [273, 2026]; [276, 2026]; [285, 2026]; [286, 2026]; [290, 2026]; [294, 2026]; [101, 2026]; [102, 2026]; [103, 2026]; [104, 2026]; [105, 2026]; [095, 2026]; [096, 2026]; [106, 2026]; [003, 2026]; [107, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 21's source-canon section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness** and [238, 2026]; [239, 2026], but only directly verified source URLs are encoded as citations.

31.3.3.3 Information Warfare and Cognitive Security intelligence practice lens: evidence artifact and safety check Practice lens: **Cognitive-Resilience Lens** for **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**. [238, 2026]; [239, 2026].

Planning question: How does the module protect autonomy, attention, trust, and decision quality without designing persuasion?

Evidence artifact: narrative-risk map with provenance, uncertainty, audience harms, and response options.

Validation rule: distinguish observation, attribution, impact assessment, and resilience response. Applied to **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**.

Handoff contract: handoff supports transparency, education, and resilience, not microtargeted influence or deception.

Safety check: exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning.

31.3.3.4 Information Warfare and Cognitive Security runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 31; [238, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	21.99	21.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Information Warfare and Cognitive Security to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Bounded autonomy, procurement, incident-response, and assurance studio	21.101	21.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Information Warfare and Cognitive Security	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Model-card, recoverability, retention, and learner-support evidence package	21.102	21.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Information Warfare and Cognitive Security	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Information Warfare Doctrine: Definitions, Theory, Air Force Policy	21.1	21.1 Information Warfare Doctrine: Definitions, Theory, Air Force Policy	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Military Deception: Six Principles and Historical Effectiveness	21.2	21.2 Military Deception: Six Principles and Historical Effectiveness	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Automated Influence and the Cognitive Security Challenge	21.3	21.3 Automated Influence and the Cognitive Security Challenge	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Cognitive Security in the Age of AI: NATO/EU Paradigm Shift	21.4	21.4 Cognitive Security in the Age of AI: NATO/EU Paradigm Shift	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Epistemic Chaos as an Adversarial Goal	21.5	21.5 Epistemic Chaos as an Adversarial Goal	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Active Inference and Predictive Processing as Models for Cognitive Attack/Defense	21.6	21.6 Active Inference and Predictive Processing as Models for Cognitive Attack/Defense	Active-Inference Boundary Lens	theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition	reject claims that the free-energy principle proves autonomous agency, intent, detection performance, or oversight-free action
Behavioral Outcomes of Human Cognitive Security (arXiv 2026)	21.7	21.7 Behavioral Outcomes of Human Cognitive Security (arXiv 2026)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning

31.3.3.5 Information Warfare and Cognitive Security reusable subsection contract: topic rows, artifacts, and safety duties **Evidence anchor.** Section 31; [238, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Information Warfare Doctrine: Definitions, Theory, Air Force Policy	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Military Deception: Six Principles and Historical Effectiveness	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Automated Influence and the Cognitive Security Challenge	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Cognitive Security in the Age of AI: NATO/EU Paradigm Shift	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Epistemic Chaos as an Adversarial Goal	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Active Inference and Predictive Processing as Models for Cognitive Attack/Defense	Active-Inference Boundary Lens	theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition	reject claims that the free-energy principle proves autonomous agency, intent, detection performance, or oversight-free action
Behavioral Outcomes of Human Cognitive Security (arXiv 2026)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning

31.3.3.6 Information Warfare and Cognitive Security annotated source ledger: real titles and local contribution Each source cited by this **Cognitive Security and Influence Resilience** module is paired below with its real title and a one-line note on what it contributes to **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**.

Source	Cited work	What it contributes	Status
[238, 2026]	Recommendation on the Ethics of Artificial Intelligence	The official UNESCO page for the Recommendation on the Ethics of Artificial Intelligence, the first global standard-setting instrument on AI ethics, adopted in 2021 and applicable to all 194 member states. It outlines four core values, including human rights protection and environmental flourishing, and ten guiding principles such as proportionality, privacy, transparency, and fairness.	verified source-guide
[239, 2026]	Digital Space and Human Rights	Official OHCHR digital rights portal.	original source-guide
[244, 2026]	AI and Education	Official UNESCO GEM AI and education source hub.	original source-guide
[273, 2026]	WCAG 2 Overview	The W3C Web Accessibility Initiative overview of the Web Content Accessibility Guidelines (WCAG), an international standard for making web content accessible to people with disabilities. It explains that WCAG is organized around four principles (perceivable, operable, understandable, robust) with testable success criteria at three conformance levels (A, AA, AAA), and covers versions 2.0, 2.1, and 2.2.	verified source-guide
[276, 2026]	What is a Data Protection Impact Assessment and When Is This Mandatory?	A European Data Protection Board FAQ page, part of its data protection guide for small businesses, explaining Data Protection Impact Assessments (DPIAs) and when they are mandatory. It describes a DPIA as a written assessment of the impact of a planned processing operation, required when processing poses high risks to individuals' rights.	verified source-guide
[285, 2026]	NIST AI Resource Center	The NIST AI Resource Center (AIRC), a government platform supporting implementation of the NIST AI Risk Management Framework, a voluntary framework for managing AI risk. It provides the core framework along with a playbook of practical actions, profiles tailored to specific sectors and technologies, use cases, and crosswalks linking the framework to other governance structures.	verified source-guide
[286, 2026]	Model Cards for Model Reporting	The arXiv abstract for "Model Cards for Model Reporting" (2018) by Mitchell, Wu, Zaldivar, and colleagues, which introduces a framework for transparent documentation of machine learning models. Model cards are short accompanying documents that report a model's benchmarked performance across varied conditions, including different cultural, demographic, and phenotypic groups, along with intended use, evaluation methodology, and deployment considerations.	verified source-guide

Source	Cited work	What it contributes	Status
[290, 2026]	NIST SP 800-218A: Secure Software Development Practices for Generative AI and Dual-Use Foundation Models	NIST Special Publication 800-218A (July 2024), which augments the Secure Software Development Framework with practices specific to AI model development across the software lifecycle. Produced in response to Executive Order 14110, it addresses AI model producers, developers building on those models, and acquirers of AI systems, and is designed to be used alongside NIST SP 800-218.	verified source-guide
[294, 2026]	M-25-21: Accelerating Federal Use of AI through Innovation, Governance, and Public Trust	An April 2025 Office of Management and Budget memorandum (M-25-21) directing executive branch agencies on federal use of artificial intelligence. Issued under Executive Order 14179, it instructs agencies to accelerate adoption of AI to improve public services and government efficiency while maintaining safeguards for civil rights, civil liberties, and privacy.	verified source-guide
[101, 2026]	Information Warfare: An Air Force Policy for the Role of Public Affairs	The military's use or misuse of information in psychological or deception operations, under.	original source-guide
[102, 2026]	Information Warfare and Deception	A 2006 paper by William Hutchinson published in the journal Informing Science. It examines the history of information warfare and the increasingly central role of deception within it, tracing the concept from its late-1980s origins as a technology-oriented military tactic for command-and-control dominance to a broader recognition of information itself as both weapon and target.	verified source-guide
[103, 2026]	Military Deception	A topic page from the Journal of Information Warfare collecting scholarly articles on military deception. Featured pieces argue that information operations officers should be conceptualized primarily as deception officers, and one quantitative reassessment reports that deception is employed in roughly 30 to 53 percent of military operations.	verified source-guide
[104, 2026]	The Utility of Military Deception and Information Operations	An essay published in Small Wars Journal (June 2025) by a U.S. Army Civil Affairs officer arguing that military deception and information operations have become central to modern conflict.	verified source-guide
[105, 2026]	Automated influence and the challenge of cognitive security	Sarah Rajtmajer and Daniel Susser, 'Automated Influence and the Challenge of Cognitive Security,' in Hot Topics in the Science of Security (HotSoS '20), April 2020, ACM. The paper argues that AI-powered computational propaganda poses national security threats that existing ethical frameworks do not address, and proposes 'cognitive security' as a productive conceptual lens for evaluating the ethics of automated influence operations and potential defensive responses.	verified source-guide
[095, 2026]	COGNITIVE SECURITY IN THE AGE OF AI	This policy paper examines the emergence of cognitive security.	original source-guide

Source	Cited work	What it contributes	Status
[096, 2026]	AI DEVELOPMENT SHOULD PRIORITIZE COGNITIVE SECURITY	A position paper (Stanford authors, ICLR 2026 workshop) arguing that AI research and development should prioritize cognitive security, defined as protecting human cognitive processes from hazardous influence. It notes that generative AI systems increasingly designed to influence beliefs and behavior raise acute governance concerns, while research on these effects remains fragmented.	verified source-guide
[106, 2026]	Applications of The Active Inference and The Free-Energy Principle	A 2024 bachelor's thesis by Lara Sakarya at Delft University of Technology presenting a systematic literature review of the active inference framework and the free-energy principle as applied to mimicking social human behavior in intelligent agents. It explains active inference as a theory describing behavior that minimizes surprise, and surveys model variants such as deep active inference, multimodal deep belief networks, predictive coding, and probabilistic programming.	verified source-guide
[003, 2026]	Active Inference: Applicability to Different Types of Social	A 2021 peer-reviewed article by Stephen Fox in the journal Entropy that relates the active inference framework to social organization. It maps concepts such as variational free energy, prediction error, generative models, and Markov blankets onto industrial engineering and quality management practices, treating organizational survival as the maintenance of process control limits.	verified source-guide
[107, 2026]	Behavioral Outcomes of Human Cognitive Security	An arXiv research paper (March 2026) proposing an integrative modeling framework for human cognitive security, defined as the degree to which people rely on truthful information to make truth-aligned judgments. It synthesizes Bayesian belief-updating with Prospect Theory to model how cognitive resources and emotional valuation shape behavior, and identifies three observable outcomes: veracity discernment, task-oriented actions, and information sharing.	verified source-guide

Where this sits. This module's overview is Section 31; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

31.3.4 Information Warfare and Cognitive Security governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 31; [238, 2026].

31.3.5 Information Warfare and Cognitive Security analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 21's governance-boundary section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **Cognitive Security and Influence Resilience** for **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**. [238, 2026]; [239, 2026].

Curriculum topic spine: Information Warfare Doctrine: Definitions, Theory, Air Force Policy, **Military Deception: Six Principles and Historical Effectiveness**, **Automated Influence and the Cognitive Security Challenge**. **Verified anchor cluster:** [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]; [OECD, 2026c]; [for Security Policy, 2025]; [Community, 2020a].

Conceptual depth: protecting attention, belief formation, and decision quality without turning resilience education into manipulation.

Method stack: claim decomposition, narrative provenance, inoculation framing, bias checks, audience-risk review, and after-action learning.

Composability contract: separate descriptive analysis, normative assessment, response options, and protected-audience considerations.

Known failure modes: counter-messaging as manipulation, overclaiming intent, pathologizing audiences, and collapsing uncertainty into moral certainty.

Defensive boundary: practice uses benign simulations and resilience education; it does not create persuasion campaigns, impersonation, or deception plans. Applied to **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**.

Anchor	Why it matters here
[Cybersecurity and Agency, 2024b]	Official CISA guidance on foreign influence operations targeting critical infrastructure. Checked as of 2026-05-21; role: source_quality_anchor.
[Organization, 2026b]	Official NATO counter-information-threat guidance. Checked as of 2026-05-21; role: source_quality_anchor.
[Cybersecurity and Agency, 2026b]	Official CISA election-security source for public-resilience, foreign-influence awareness, rumor control, and defensive communication framing. Checked as of 2026-05-21; role: curriculum_anchor.
[Organization, 2026c]	Official NATO source for hybrid-threat resilience across cyber, information, economic, political, and military pressure. Checked as of 2026-05-21; role: curriculum_anchor.
[OECD, 2026c]	Official OECD policy source for information integrity, governance responses, public trust, and democratic resilience. Checked as of 2026-05-21; role: curriculum_anchor.
[for Security Policy, 2025]	Policy-scholarship source for cognitive security, information literacy, critical thinking, and whole-of-society resilience. Checked as of 2026-05-21; role: curriculum_anchor.
[Community, 2020a]	Official IC framework for AI goals, authorities, human judgment, bias mitigation, testing, documentation, explainability, and review. Checked as of 2026-05-21; role: curriculum_anchor.

31.3.5.1 Information Warfare and Cognitive Security evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **Cognitive Security and Influence Resilience** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [238, 2026]; [239, 2026].

31.3.6 Information Warfare and Cognitive Security agentic boundary: assist, approve, block, and record

Evidence anchor. Section 31; [238, 2026].

AGEINT translation is bounded by the **Cognitive Security and Influence Resilience** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**.

31.3.6.1 Information Warfare and Cognitive Security permitted defensive utility: curriculum uses and safe outputs Evidence anchor. Section 31; [238, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**.

31.3.6.2 Information Warfare and Cognitive Security excluded operational boundary: blocked actions and stop rules Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [238, 2026]; [239, 2026] and **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

31.3.7 Information Warfare and Cognitive Security governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 31; [238, 2026].

Governance is practiced as a gate on the **Cognitive Security and Influence Resilience** lane. Learners use the **Cognitive-Resilience Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**.

31.3.7.1 Information Warfare and Cognitive Security governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [238, 2026]; [239, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Cognitive Security and Influence Resilience** failure modes and the **Cognitive-Resilience Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

31.3.7.2 Information Warfare and Cognitive Security evidence package handoff: appendices, records, and reuse

Evidence anchor. Section 31; [238, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Cognitive-Resilience Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**.

31.3.7.3 Information Warfare and Cognitive Security current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**. [238, 2026]; [239, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_cisa_foreign_influence` for **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**?	Preparing for and Mitigating Foreign Influence Operations; lane `source_quality_spine`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official CISA guidance on foreign influence operations targeting critical infrastructure.
What does the module inherit from `official_nato_counter_information_threats` for **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**?	Countering Information Threats; lane `source_quality_spine`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official NATO counter-information-threat guidance.
What does the module inherit from `official_cisa_election_security_influence` for **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**?	Election Security; lane `cognitive_influence_security`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official CISA election-security source for public-resilience, foreign-influence awareness, rumor control, and defensive communication framing.
What does the module inherit from `official_nato_hybrid_threats` for **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**?	Countering Hybrid Threats; lane `cognitive_influence_security`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official NATO source for hybrid-threat resilience across cyber, information, economic, political, and military pressure.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 31; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

31.3.8 Information Warfare and Cognitive Security assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 31; [238, 2026].

31.3.9 Information Warfare and Cognitive Security assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 31; [238, 2026].

31.3.9.1 Information Warfare and Cognitive Security capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**.
Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness** and [238, 2026]; [239, 2026].

31.3.9.2 Information Warfare and Cognitive Security instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness** and [238, 2026]; [239, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

31.3.9.3 Information Warfare and Cognitive Security assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Information Warfare Doctrine: Definitions, Theory, Air Force Policy	Completed **narrative-risk map with provenance, uncertainty, audience harms, and response options** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Military Deception: Six Principles and Historical Effectiveness	Completed **narrative-risk map with provenance, uncertainty, audience harms, and response options** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Automated Influence and the Cognitive Security Challenge	Completed **narrative-risk map with provenance, uncertainty, audience harms, and response options** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

31.3.10 Information Warfare and Cognitive Security refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [238, 2026]; [239, 2026] and **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**.

31.3.10.1 Information Warfare and Cognitive Security refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**. The local signals begin with [238, 2026]; [239, 2026].

31.3.10.2 Information Warfare and Cognitive Security claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**, and the source spine for these checks begins with [238, 2026]; [239, 2026].

31.3.11 Information Warfare and Cognitive Security reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [238, 2026]; [239, 2026].
Triangulation anchors. In module 21's review-checklist section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness**. [238, 2026]; [239, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

31.3.12 Information Warfare and Cognitive Security learning-path links: module map, overview, and curriculum atlas

These links keep **Information Warfare Doctrine: Definitions, Theory, Air Force Policy; Military Deception: Six Principles and Historical Effectiveness** paired with the orientation atlas, the parent unit, and the previous and next modules, so a reader can trace which claims and caveats are inherited rather than re-derived here. Anchored at [238, 2026]; [239, 2026].

Section 2, Section 27, Section 30, Section 32

32 COUNTERINTELLIGENCE

32.1 COUNTERINTELLIGENCE learning spine and source route: unit purpose, module order, and evidence handoff

Evidence anchor. Section 32; [238, 2026].

32.1.1 source-integrity defense discipline spine: domain question and learning focus

Evidence anchor. Section 32; [238, 2026].
This unit teaches **source-integrity defense**. CI lessons teach deception awareness, source integrity, insider-risk signals, corroboration, and protected escalation as defensive governance.

32.1.2 source-integrity defense source-use contract: citation roles and evidence limits

Evidence anchor. Section 32; [238, 2026].
Use guide citations and analytic-standards anchors to ground claims about deception, corroboration, uncertainty, and review.

32.1.3 source-integrity defense practice artifact: recurring packet and retained evidence

Evidence anchor. Section 32; [238, 2026].
The recurring practice artifact is a **source-integrity challenge memo** that draws on anomaly hypothesis table, corroboration note, protected-disclosure path, and uncertainty statement. The unit keeps its learning spine explicit. Learners list competing explanations for compromise signals and preserve uncertainty until evidence justifies escalation.

32.1.4 source-integrity defense safety boundary: accountable, synthetic, and evidence-bounded limits

No surveillance, cover construction, handling, elicitation, or operational security playbooks.
This unit introduces the part's governing question, evidence artifacts, source-support spine, and capstone thread before the individual modules begin. [238, 2026]; [240, 2026].
Learners carry one unit capstone thread through the part: define an accountable intelligence question, bind it to source-quality constraints, produce a reviewable artifact, test the artifact against failure modes, and hand it off with enough context for another analyst or instructor to audit. The capstone remains public, synthetic, or owned-lab throughout; its first source anchors are [238, 2026]; [240, 2026].
This unit's deliverables are a source-canon card, claim/evidence ledger, safe-practice lab packet, failure-mode note, instructor rubric, and debrief memo. The full source-lane and evidence-package ledgers appear in the orientation and appendices; this unit introduction keeps only the learner-facing spine for [238, 2026]; [240, 2026].
This unit's safety gates are scope authorization, rights review, data provenance, tool allowlisting, human oversight, rollback, and evidence-bounded output. A missing gate turns the activity into a tabletop, audit, or written governance exercise until the gate is restored against [238, 2026]; [240, 2026].
Capstone thread:

Phase	Artifact	Review gate
Question	accountable learning question and excluded-action list	instructor confirms scope, allowed data, and rights impact
Source canon	source-lane map with guide citations, verified anchors, and refresh dates	citation keys resolve and source identity lock remains stable
Evidence ledger	claim, evidence, uncertainty, confidence, and reviewer register	every material claim has a source, caveat, and owner
Safe lab	synthetic or public dataset packet, tool allowlist, and stop conditions	no live target, private data, external action, or unsafe cyber-physical step
Assurance	evaluation rubric, failure-mode drill, rights map, and remediation note	human reviewer signs off before presentation or reuse
Debrief	capstone memo with lessons, residual risk, refresh triggers, and handoff owner	all unresolved questions and future approvals are explicit

Research lane: Counterintelligence and Source-Integrity Defense. Core anchors: [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]. Conceptual focus: defending institutions, sources, and judgments against deception, insider risk, foreign-intelligence targeting, and source contamination. Composability contract: identity, access, reporting, corroboration, caveats, and confidence are modeled independently so defensive review can happen without exposure. **Practice lens:** Structured-Judgment Lens; Which assumptions, alternatives, confidence statements, and source limits must stay visible for review? [238, 2026]; [240, 2026].

32.1.5 COUNTERINTELLIGENCE visual navigation and module map: evidence flow, order, and safety cues

The unit uses Figure 70 and Figure 71 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 31, Section 33.

32.1.6 COUNTERINTELLIGENCE module roster and source-lane inventory: citations, lanes, and learner route

Module	Section reference	Source spine
Counterintelligence Fundamentals	Section 33	[238, 2026]; [240, 2026]; [241, 2026]; [274, 2026]; [278, 2026]; [280, 2026]; [287, 2026]; [288, 2026]; [295, 2026]; [012, 2026]; [108, 2026]; [029, 2026]; [297, 2026]; [298, 2026].
Counterintelligence Against Non-State Actors	Section 34	[239, 2026]; [240, 2026]; [241, 2026]; [279, 2026]; [282, 2026]; [284, 2026]; [289, 2026]; [291, 2026]; [296, 2026]; [012, 2026]; [033, 2026]; [109, 2026]; [307, 2026]; [305, 2026]; [304, 2026].

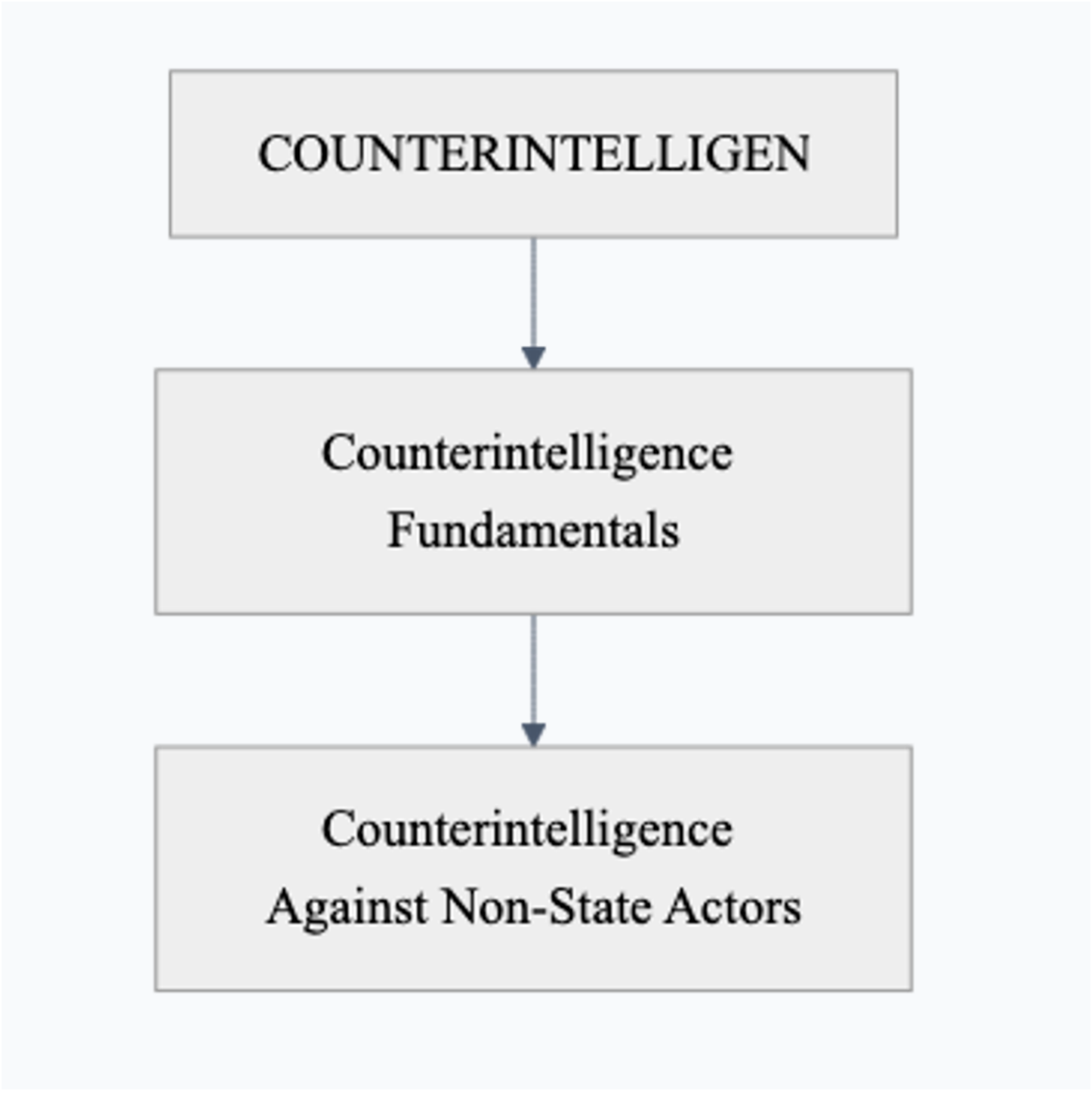


Figure 70: The unit module map traces the part's chapters as a linear reading sequence. In the counterintelligence section, it lets readers compare 2 module nodes in the unit's ordered, source-backed reading sequence from its first module to its last so the visual functions as a traceable course aid rather than an unscoped assertion.

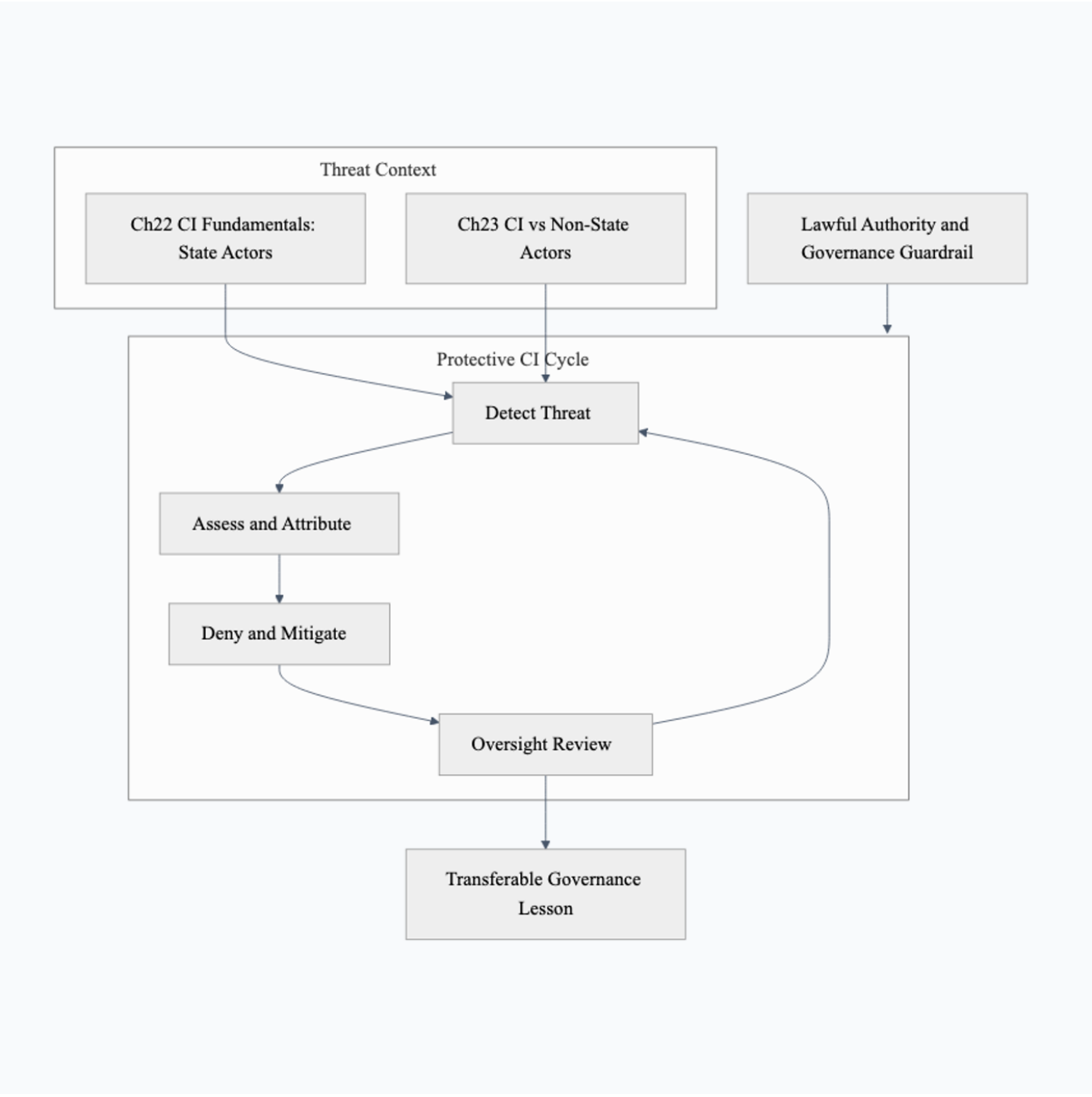


Figure 71: This Part presents counterintelligence as a continuous protective cycle whose detect-assess-deny-review loop is applied across both state and non-state adversaries. Its reader value is to make Threat Context, Ch22 CI Fundamentals: State Actors, Ch23 CI vs Non-State Actors, and Protective CI Cycle visible at a glance, with the counterintelligence section as the source section and defensive review as the boundary.

33 Counterintelligence Fundamentals

33.0.1 Counterintelligence Fundamentals figures and course links: visual evidence, source flow, and navigation

The module uses Figure 72 and Figure 70 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 32, Section 34.
This module teaches the **Counterintelligence and Source-Integrity Defense** lane through a bounded, source-backed coursebook chapter. [238, 2026]; [240, 2026].

33.1 Counterintelligence and Source-Integrity Defense frame for Counterintelligence Fundamentals: source context, topic focus, and reader task

Evidence anchor. Section 33; [238, 2026].

33.1.1 Counterintelligence Fundamentals orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 33; [238, 2026].

33.1.2 Counterintelligence Fundamentals conceptual primer: source context, core model, and reader task

This chapter teaches counterintelligence as source-integrity defense: the class studies how institutions protect evidence, people, access, and judgment from deception and compromise. The chapter uses **Structured-Judgment Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**.
The central distinction is to separate defensive awareness from surveillance, handling, or operational security playbooks. Core topics include **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records; Insider Threat Analysis: Source-vetting and insider-threat review using sample personnel records**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [238, 2026]; [240, 2026].
Learners move from vocabulary and the **Structured-Judgment Lens** distinction through topic lessons on **Source-vetting and insider-threat review using sample personnel records** with evidence and misconception checks, then assemble an **analytic note with hypotheses, evidence table, confidence, and dissent fields** with safety and rights gates.

33.1.3 Counterintelligence Fundamentals learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 33; [238, 2026].

- Connect **Source-vetting and insider-threat review using sample personnel records and Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records** to **Counterintelligence and Source-Integrity Defense** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build an **analytic note with hypotheses, evidence table, confidence, and dissent fields** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate defensive awareness from surveillance, handling, or operational security playbooks; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as source compromise, deception acceptance, identity overconfidence, insider blind spots, and collapsing CI concerns into undifferentiated IT-security triage, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: CI content supports defensive awareness, source protection, and analytic integrity; it does not provide surveillance or handling playbooks.

33.1.4 Counterintelligence Fundamentals core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 33; [238, 2026].

Term	Working definition
Source integrity	confidence that evidence has not been distorted, laundered, or compromised
Compromise signal	a clue that access, identity, or source reliability needs review
Corroboration	independent support that reduces single-source vulnerability
Insider risk	risk created by trusted access combined with motive, pressure, or control failure
Protected disclosure	a safe channel for reporting concerns without exposing sensitive details
Source-vetting and insider-threat review using…	Key terms: vetting, insider, threat.
Offensive vs Defensive Counterintelligence:…	Key terms: Offensive, Defensive, Counterintelligence.

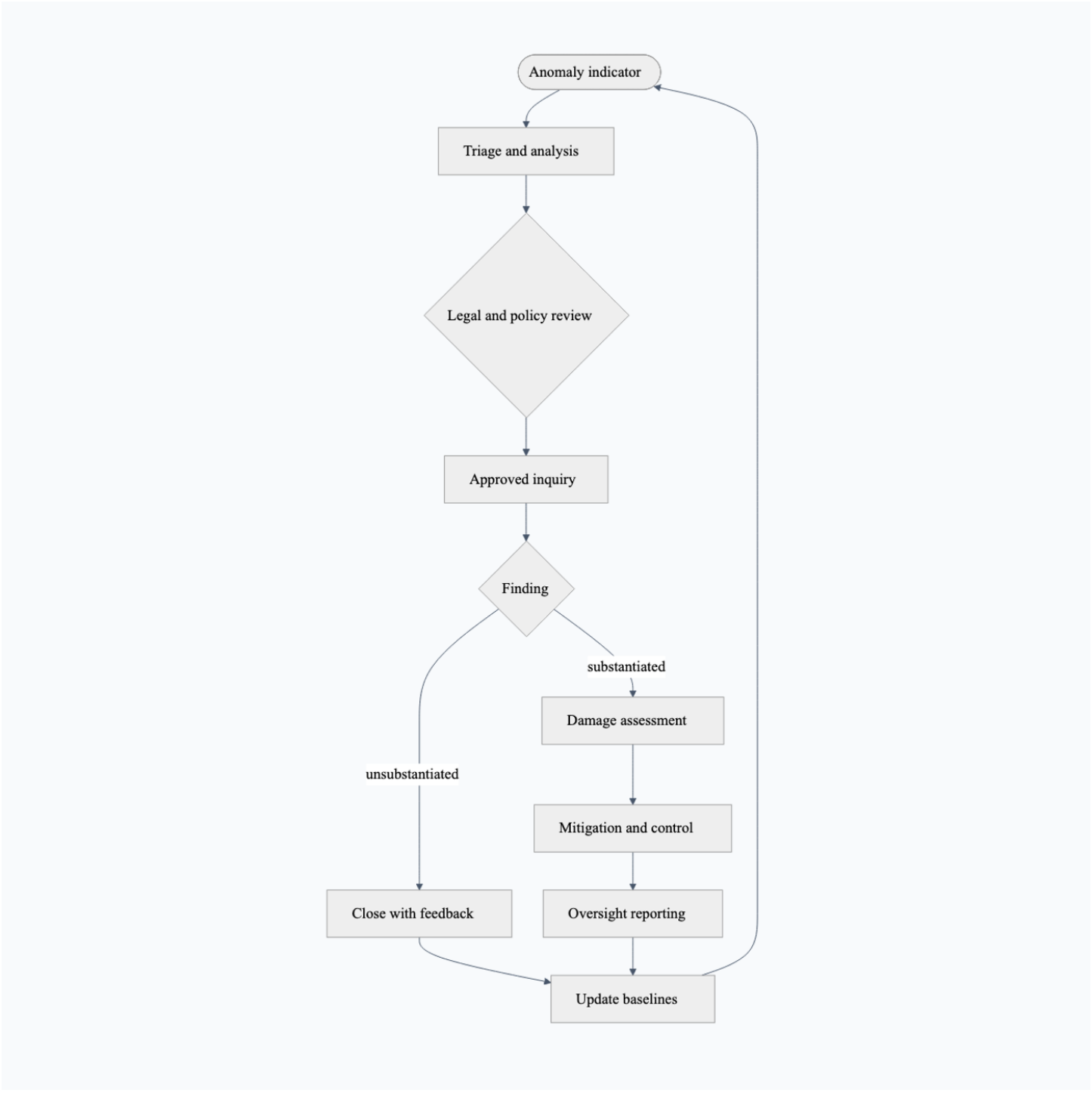


Figure 72: The oversight-bounded cycle by which an anomaly indicator becomes a governed counterintelligence investigation with damage assessment and legal review at every gate. The captioned view belongs to the counterintelligence / counterintelligence fundamentals section and should be read as a map of Anomaly indicator, Triage and analysis, Approved inquiry, and Close with feedback, not as a capability score or live-task instruction.

33.2 Structured-Judgment Lens path for Counterintelligence Fundamentals: lesson cluster, safe artifact, and review

Evidence anchor. Section 33; [238, 2026].

33.2.1 Counterintelligence Fundamentals practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 33; [238, 2026].

33.2.2 Counterintelligence Fundamentals topic lessons: source-backed concepts and transfer tasks

This module builds counterintelligence as source-integrity defense: the class studies how institutions protect evidence, people, access, and judgment from deception and compromise. The sequence opens with **Source-vetting and insider-threat review using sample personnel records**, **Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**, **Insider Threat Analysis: Source-vetting and insider-threat review using sample personnel records** and applies the **Structured-Judgment Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 70; module overview Section 33; curriculum atlas Section 2.

Triangulation anchors. In module 22's topic-lessons section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

33.2.2.1 Lesson 1: Source-vetting and insider-threat review using sample personnel records Concept. Source-vetting and insider-threat review using sample personnel records connects insider-threat review to access control, behavior indicators, and accountable escalation paths.

Why it matters. Analysts use **Source-vetting and insider-threat review using sample personnel records** to separate defensive awareness from surveillance, handling, or operational security playbooks. A defensible treatment names the judgment it enables for deception-aware source review and defensive escalation review, the proof limit that source compromise would otherwise hide, and the reviewer accountable for challenge.

Source support. Source-vetting and insider-threat review using sample personnel records rests on [012, 2026]. Its anchor reference records: A Grey Dynamics analysis article (Rachel Brown, 2021) on how non-state actors conduct counterintelligence. Use it for the claim that **Source-vetting and insider-threat review using sample personnel records** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. Read **Source-vetting and insider-threat review using sample personnel records** against the works cited for this row. [012, 2026] A Grey Dynamics analysis article (Rachel Brown, 2021) on how non-state actors conduct counterintelligence. It argues that although such groups lack the technical collection capabilities of states, they compensate through open-source and human-source methods and benefit defensively from compartmentalized, cell-based structures and ideological cohesion. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Source-vetting and insider-threat review using sample personnel records**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this deception-aware source review and defensive escalation topic. The artifact must record the vetting descriptor, the bounded claim about **Source-vetting and insider-threat review using**, the bias caveat, the uncertainty note, the unproven-allegation boundary, and the reviewer who adjudicates. Shape this subject work as a **source-integrity challenge memo** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Source-vetting and insider-threat review using sample personnel records**: that a clean vetting result certifies present trustworthiness rather than a point-in-time judgment that must be continuously re-examined.

Transfer task. Reuse the **Source-vetting and insider-threat review using sample personnel records** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

33.2.2.2 Lesson 2: Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records Concept. Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records frames counterintelligence as source-vetting, anomaly review, and institutional protection—not operational entrapment.

Why it matters. Offensive vs Defensive Counterintelligence connects classroom vocabulary to Counterintelligence and Source-Integrity Defense practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records rests on [012, 2026]. The most specific cited work observes: It argues that although such groups lack the technical collection capabilities of states, they compensate through open-source and human-source methods and benefit defensively from compartmentalized, cell-based structures and ideological cohesion. Use it for the claim that **Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. For **Offensive vs Defensive Counterintelligence**, work from the cited evidence behind this row. [012, 2026] A Grey Dynamics analysis article (Rachel Brown, 2021) on how non-state actors conduct counterintelligence. It argues that although such groups lack the technical collection capabilities of states, they compensate through open-source and human-source methods and benefit defensively from compartmentalized, cell-based structures and ideological cohesion. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Offensive vs Defensive Counterintelligence**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this deception-aware source review and defensive escalation topic. The artifact must record the vetting descriptor, the bounded claim about **Offensive vs Defensive Counterintelligence**, the bias caveat, the uncertainty note, the unproven-allegation boundary, and the reviewer who adjudicates. Shape **Offensive vs Defensive Counterintelligence** work as a **source-integrity challenge memo** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Offensive vs Defensive Counterintelligence**: that a clean vetting result certifies present trustworthiness rather than a point-in-time judgment that must be continuously re-examined.

Transfer task. Transfer **Offensive vs Defensive Counterintelligence** from this module to a second motif by preserving deception-aware source review and defensive escalation, replacing action with audit, and naming the blocked use.

33.2.2.3 Lesson 3: Insider Threat Analysis: Source-vetting and insider-threat review using sample personnel records Concept. Insider Threat Analysis: Source-vetting and insider-threat review using sample personnel records connects insider-threat review to access control, behavior indicators, and accountable escalation paths.

Why it matters. Without explicit treatment of **Insider Threat Analysis**, source compromise undermines deception-aware source review and defensive escalation review; the lesson builds the habit to separate defensive awareness from surveillance, handling, or operational security playbooks.

Source support. Insider Threat Analysis: Source-vetting and insider-threat review using sample personnel records rests on [108, 2026]. The closest source to this row notes: Intelligence Analysis. Use it for pinning down the scope of **Insider Threat Analysis: Source-vetting and insider-threat review using sample personnel records**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. For **Insider Threat Analysis**, work from the cited evidence behind this row. [108, 2026] A Tradecraft Primer: Structured Analytic Techniques for Improving. Intelligence Analysis. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Insider Threat Analysis**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this deception-aware source review and defensive escalation topic. The artifact must record the vetting descriptor, the bounded claim about **Insider Threat Analysis**, the bias caveat, the uncertainty note, the unproven-allegation boundary, and the reviewer who adjudicates. Shape **Insider Threat Analysis** work as a **source-integrity challenge memo** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Insider Threat Analysis**: that a clean vetting result certifies present trustworthiness rather than a point-in-time judgment that must be continuously re-examined.

Transfer task. Reuse the **Insider Threat Analysis** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

33.2.2.4 Lesson 4: Double-Agent and Triple-Cross Operations: Source-vetting and insider-threat review using sample personnel records

Concept. Double-Agent and Triple-Cross Operations: Source-vetting and insider-threat review using sample personnel records connects insider-threat review to access control, behavior indicators, and accountable escalation paths.

Why it matters. Double-Agent and Triple-Cross Operations matters in the **Counterintelligence and Source-Integrity Defense** lane because deception-aware source review and defensive escalation evidence must stay separate from judgment; source compromise is a common failure.

Source support. Double-Agent and Triple-Cross Operations: Source-vetting and insider-threat review using sample personnel records rests on [012, 2026] and [029, 2026]. The closest source to this row notes: It surveys the roles of case officers in managing sources, recruitment and training of agents, protective measures such as fronts and cutouts, agent classifications including unwitting sources, and counterintelligence methods for identifying foreign operatives and reducing security breaches. Use them for the claim that **Double-Agent and Triple-Cross Operations: Source-vetting and insider-threat review using sample personnel records** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. For **Double-Agent and Triple-Cross Operations**, work from the cited evidence behind this row. [012, 2026] A Grey Dynamics analysis article (Rachel Brown, 2021) on how non-state actors conduct counterintelligence. It argues that although such groups lack the technical collection capabilities of states, they compensate through open-source and human-source methods and benefit defensively from compartmentalized, cell-based structures and ideological cohesion. [029, 2026] A roughly 28-page Scribd document titled "Agent Handling in Counterintelligence" providing an educational overview of intelligence operations. It surveys the roles of case officers in managing sources, recruitment and training of agents, protective measures such as fronts and cutouts, agent classifications including unwitting sources, and counterintelligence methods for identifying foreign operatives and reducing security breaches. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Double-Agent and Triple-Cross Operations**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this deception-aware source review and defensive escalation topic. The artifact must record the vetting descriptor, the bounded claim about **Double-Agent and Triple-Cross Operations**, the bias caveat, the uncertainty note, the unproven-allegation boundary, and the reviewer who adjudicates. Shape **Double-Agent and Triple-Cross Operations** work as a **source-integrity challenge memo** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Double-Agent and Triple-Cross Operations**: that a clean vetting result certifies present trustworthiness rather than a point-in-time judgment that must be continuously re-examined.

Transfer task. Apply this module's safe boundary for **Double-Agent and Triple-Cross Operations** to another artifact while keeping deception-aware source review and defensive escalation and reviewer ownership explicit.

33.2.2.5 Lesson 5: Penetration of Hostile Services: Source-vetting and insider-threat review using sample personnel records

Concept. Penetration of Hostile Services: Source-vetting and insider-threat review using sample personnel records connects insider-threat review to access control, behavior indicators, and accountable escalation paths.

Why it matters. Without explicit treatment of **Penetration of Hostile Services**, source compromise undermines deception-aware source review and defensive escalation review; the lesson builds the habit to separate defensive awareness from surveillance, handling, or operational security playbooks.

Source support. Penetration of Hostile Services: Source-vetting and insider-threat review using sample personnel records rests on [297, 2026] and [298, 2026]. The lead source's own note reads: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for fixing what **Penetration of Hostile Services: Source-vetting and insider-threat review using sample personnel records** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. For **Penetration of Hostile Services**, work from the cited evidence behind this row. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Penetration of Hostile Services**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this deception-aware source review and defensive escalation topic. The artifact must record the vetting descriptor, the bounded claim about **Penetration of Hostile Services**, the bias caveat, the uncertainty note, the unproven-allegation boundary, and the reviewer who adjudicates. Shape **Penetration of Hostile Services** work as a **source-integrity challenge memo** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Penetration of Hostile Services**: that a clean vetting result certifies present trustworthiness rather than a point-in-time judgment that must be continuously re-examined.

Transfer task. Apply this module's safe boundary for **Penetration of Hostile Services** to another artifact while keeping deception-aware source review and defensive escalation and reviewer ownership explicit.

33.2.2.6 Lesson 6: Polygraph: Source-vetting and insider-threat review using sample personnel records

Concept. Polygraph: Source-vetting and insider-threat review using sample personnel records connects insider-threat review to access control, behavior indicators, and accountable escalation paths.

Why it matters. Polygraph: Source-vetting and insider-threat review using sample personnel records connects classroom vocabulary to Counterintelligence and Source-Integrity Defense practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Polygraph: Source-vetting and insider-threat review using sample personnel records rests on [297, 2026] and [298, 2026]. The closest source to this row notes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence,

timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for the claim that **Polygraph: Source-vetting and insider-threat review using sample personnel records** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. Read **Polygraph: Source-vetting and insider-threat review using sample personnel records** against the works cited for this row. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Polygraph**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this deception-aware source review and defensive escalation topic. The artifact must record the vetting descriptor, the bounded claim about **Polygraph**, the bias caveat, the uncertainty note, the unproven-allegation boundary, and the reviewer who adjudicates. Shape **Polygraph: Source-vetting and insider-threat review using sample personnel records** work as a **source-integrity challenge memo** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Polygraph: Source-vetting and insider-threat review using sample personnel records**: that a clean vetting result certifies present trustworthiness rather than a point-in-time judgment that must be continuously re-examined.

Transfer task. Apply this module's safe boundary for **Polygraph: Source-vetting and insider-threat review using sample personnel records** to another artifact while keeping deception-aware source review and defensive escalation and reviewer ownership explicit.

33.2.2.7 Lesson 7: Damage Assessment and Control: Source-vetting and insider-threat review using sample personnel records

Concept. Damage Assessment and Control: Source-vetting and insider-threat review using sample personnel records connects insider-threat review to access control, behavior indicators, and accountable escalation paths.

Why it matters. Without explicit treatment of **Damage Assessment and Control**, source compromise undermines deception-aware source review and defensive escalation review; the lesson builds the habit to separate defensive awareness from surveillance, handling, or operational security playbooks.

Source support. Damage Assessment and Control: Source-vetting and insider-threat review using sample personnel records rests on [297, 2026] and [298, 2026]. The lead source's own note reads: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for fixing what **Damage Assessment and Control: Source-vetting and insider-threat review using sample personnel records** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. For **Damage Assessment and Control**, reason from the sources cited in this row. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Damage Assessment and Control**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this deception-aware source review and defensive escalation topic. The artifact must record the vetting descriptor, the bounded claim about **Damage Assessment and Control**, the bias caveat, the uncertainty note, the unproven-allegation boundary, and the reviewer who adjudicates. Shape **Damage Assessment and Control** work as a **source-integrity challenge memo** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Damage Assessment and Control**: that a clean vetting result certifies present trustworthiness rather than a point-in-time judgment that must be continuously re-examined.

Transfer task. Apply this module's safe boundary for **Damage Assessment and Control** to another artifact while keeping deception-aware source review and defensive escalation and reviewer ownership explicit.

33.2.2.8 Lesson 8: Case Studies: Source-vetting and insider-threat review using sample personnel records

Concept. Case Studies: Source-vetting and insider-threat review using sample personnel records connects insider-threat review to access control, behavior indicators, and accountable escalation paths.

Why it matters. Analysts use **Case Studies** to separate defensive awareness from surveillance, handling, or operational security playbooks. A defensible treatment names the judgment it enables for deception-aware source review and defensive escalation review, the proof limit that source compromise would otherwise hide, and the reviewer accountable for challenge.

Source support. Case Studies: Source-vetting and insider-threat review using sample personnel records rests on [297, 2026] and [298, 2026]. The closest source to this row notes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for fixing what **Case Studies: Source-vetting and insider-threat review using sample personnel records** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. Ground **Case Studies** in the evidence the row cites. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Case Studies**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this deception-aware source review and defensive escalation topic. The artifact must record the vetting descriptor, the bounded claim about **Case Studies**, the bias caveat, the uncertainty note, the unproven-allegation boundary, and the reviewer who adjudicates. Shape **Case Studies** work as a **source-integrity challenge memo** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Case Studies**: that a clean vetting result certifies present trustworthiness rather than a point-in-time judgment that must be continuously re-examined.

Transfer task. Reuse the **Case Studies** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

33.2.3 Counterintelligence Fundamentals worked safe example: synthetic inputs, evidence, and review

Worked example: a sample research lab reviews a synthetic source-quality anomaly after a disputed report. [238, 2026]; [240, 2026].

Triangulation anchors. In module 22's worked-example section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **source-integrity defense**. Learners use a **source-integrity challenge memo** and keep this boundary visible: No surveillance, cover construction, handling, elicitation, or operational security playbooks.

Frame. The classroom question centers on **Source-vetting and insider-threat review using sample personnel records**. Excluded actions

stay explicit, and the **Structured-Judgment Lens** planning question is: Which assumptions, alternatives, confidence statements, and source limits must stay visible for review?

Inputs. For the **Source-vetting and insider-threat review using sample personnel records** scenario, use toy access logs, public policy excerpts, synthetic source notes, and a reviewer escalation path. The Structured-Judgment Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Source-vetting and insider-threat review using sample personnel records**, students separate identity from access, list anomaly hypotheses, seek corroboration, and route sensitive concerns to review. Pause whenever an inference about Source-vetting and insider-threat review using sample personnel records appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Source-vetting and insider-threat review using sample personnel records** classroom scenario; unit artifact = source-integrity challenge memo; evidence = allowed inputs; method = deception-aware source review and defensive escalation; output = a source-integrity memo with competing explanations, confidence, protected-disclosure note, and next-review owner; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Source-vetting and insider-threat review using sample personnel records** as "Structured-Judgment Lens confirms it" is not enough. The revision ties the claim to deception-aware source review and defensive escalation, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Source-vetting and insider-threat review using sample personnel records** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

33.2.4 Counterintelligence Fundamentals practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Structured-Judgment Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**.

Triangulation anchors. In module 22's practice-sequence section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Source-vetting and insider-threat review using sample personnel records, Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records, Insider Threat Analysis: Source-vetting and insider-threat review using sample personnel records; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Counterintelligence and Source-Integrity Defense** lane.
2. Frame	Answer the lens question: Which assumptions, alternatives, confidence statements, and source limits must stay visible for review?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Source-vetting and insider-threat review using sample personnel records: analytic note with hypotheses, evidence table, confidence, and dissent fields.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the source-integrity challenge memo fields for Source-vetting and insider-threat review using sample personnel records.	Unit profile note.	Evidence artifacts include anomaly hypothesis table, corroboration note.
4. Challenge	Test the misconception that a clean vetting result certifies present trustworthiness rather than a point-in-time judgment that must be continuously re-examined.	Failure-mode note.	The artifact applies the key distinction: separate defensive awareness from surveillance, handling, or operational security playbooks.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

33.2.4.1 Counterintelligence Fundamentals instructor notes: source reasoning, review points, and studio focus

Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**. [238, 2026]; [240, 2026].

33.2.4.2 Counterintelligence Fundamentals extension exercise: peer validation and refresh trigger review

Evidence anchor. Section 33; [238, 2026].

Have learners swap artifacts and apply the **Structured-Judgment Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**.

33.2.5 Counterintelligence Fundamentals knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 33; [238, 2026].

1. Explain how **Source-vetting and insider-threat review using sample personnel records** is defined here; name the source descriptor that supports the definition.

2. Contrast **Source-vetting and insider-threat review using sample personnel records** with **Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records** using the **Structured-Judgment Lens** artifact fields.
3. Identify one failure mode from the **Counterintelligence and Source-Integrity Defense** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which explanation preserves uncertainty without ignoring a possible compromise signal?
5. Correct this misconception: that a clean vetting result certifies present trustworthiness rather than a point-in-time judgment that must be continuously re-examined.

33.2.5.1 Counterintelligence Fundamentals answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Source-vetting and insider-threat review using sample personnel records** without source evidence, uncertainty, or a safe transfer task.

33.3 Counterintelligence Fundamentals assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 33; [238, 2026].

33.3.1 Counterintelligence Fundamentals evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 33; [238, 2026].

33.3.2 Counterintelligence Fundamentals transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 33; [238, 2026].

33.3.2.1 Counterintelligence Fundamentals lineage and source tradition: profile, concepts, and first anchors This sits in the **Counterintelligence and Source-Integrity Defense** lineage: defending institutions, sources, and judgments against deception, insider risk, foreign-intelligence targeting, and source contamination. [238, 2026]; [240, 2026].

33.3.2.2 Counterintelligence Fundamentals working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 33; [238, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**, with provenance and reviewability throughout.

33.3.2.3 Counterintelligence Fundamentals knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [238, 2026]; [240, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

33.3.2.4 Counterintelligence Fundamentals transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 33; [238, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**.
- **Evidence contract:** keep the **Counterintelligence and Source-Integrity Defense** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

33.3.2.5 Counterintelligence Fundamentals profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 33; [238, 2026].

The matched profile emphasizes defending institutions, sources, and judgments against deception, insider risk, foreign-intelligence targeting, and source contamination. The method stack is threat awareness, source-descriptor audit, corroboration, anomaly review, red-team challenge, and protected disclosure paths; the local topic cluster is **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**.

33.3.3 Counterintelligence Fundamentals evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 33; [238, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Counterintelligence and Source-Integrity Defense** profile tells reviewers what evidence is strong enough for the module artifact built around **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**.

33.3.3.1 Counterintelligence Fundamentals guide source spine: inherited keys and local citation roles Primary guide citations: [238, 2026]; [240, 2026]; [241, 2026]; [274, 2026]; [278, 2026]; [280, 2026]; [287, 2026]; [288, 2026]; [295, 2026]; [012, 2026]; [108, 2026]; [029, 2026]; [297, 2026]; [298, 2026].

33.3.3.2 Counterintelligence Fundamentals verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [238, 2026]; [240, 2026].

Tier	What counts	How it is used
Source guide	[238, 2026]; [240, 2026]; [241, 2026]; [274, 2026]; [278, 2026]; [280, 2026]; [287, 2026]; [288, 2026]; [295, 2026]; [012, 2026]; [108, 2026]; [029, 2026]; [297, 2026]; [298, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 22's source-canon section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records** and [238, 2026]; [240, 2026], but only directly verified source URLs are encoded as citations.

33.3.3.3 Counterintelligence Fundamentals intelligence practice lens: evidence artifact and safety check Practice lens: **Structured-Judgment Lens** for **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**. [238, 2026]; [240, 2026].

Planning question: Which assumptions, alternatives, confidence statements, and source limits must stay visible for review?

Evidence artifact: analytic note with hypotheses, evidence table, confidence, and dissent fields.

Validation rule: separate raw reporting, inference, judgment, and recommendation before synthesis. Applied to **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**.

Handoff contract: handoff preserves alternatives, uncertainty, caveats, and revision history for downstream modules.

Safety check: avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence.

33.3.3.4 Counterintelligence Fundamentals runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 33; [238, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	22.99	22.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Counterintelligence Fundamentals to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Bounded autonomy, procurement, incident-response, and assurance studio	22.101	22.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Counterintelligence Fundamentals	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Model-card, recoverability, retention, and learner-support evidence package	22.102	22.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Counterintelligence Fundamentals	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Source-vetting and insider-threat review using sample personnel records	22.1	22.1 source title transformed into safe curriculum treatment; original: CI Definition, Scope, Relationship to Intelligence	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-vetting and insider-threat review using sample personnel records	22.2	22.2 source title transformed into safe curriculum treatment; original: Offensive vs. Defensive Counterintelligence	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Source-vetting and insider-threat review using sample personnel records	22.3	22.3 source title transformed into safe curriculum treatment; original: Insider Threat Analysis: Critical Thinking Techniques (CDSE)	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Source-vetting and insider-threat review using sample personnel records	22.4	22.4 source title transformed into safe curriculum treatment; original: The Double-Agent and Triple-Cross Operations	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Source-vetting and insider-threat review using sample personnel records	22.5	22.5 source title transformed into safe curriculum treatment; original: Penetration of Hostile Services	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Source-vetting and insider-threat review using sample personnel records	22.6	22.6 source title transformed into safe curriculum treatment; original: Polygraph: Use and Limitations in CI	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Source-vetting and insider-threat review using sample personnel records	22.7	22.7 source title transformed into safe curriculum treatment; original: Damage Assessment and Control	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Source-vetting and insider-threat review using sample personnel records	22.8	22.8 source title transformed into safe curriculum treatment; original: Case Studies: Hanssen, Ames, Lee, Pollard	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

33.3.3.5 Counterintelligence Fundamentals reusable subsection contract: topic rows, artifacts, and safety duties **Evidence anchor.** Section 33; [238, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Source-vetting and insider-threat review using sample personnel records	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Insider Threat Analysis: Source-vetting and insider-threat review using sample personnel records	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Double-Agent and Triple-Cross Operations: Source-vetting and insider-threat review using sample personnel records	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Penetration of Hostile Services: Source-vetting and insider-threat review using sample personnel records	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Polygraph: Source-vetting and insider-threat review using sample personnel records	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Damage Assessment and Control: Source-vetting and insider-threat review using sample personnel records	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence

Lesson topic	Practice lens	Evidence artifact	Safety check
Case Studies: Source-vetting and insider-threat review using sample personnel records	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

33.3.3.6 Counterintelligence Fundamentals annotated source ledger: real titles and local contribution Each source cited by this **Counterintelligence and Source-Integrity Defense** module is paired below with its real title and a one-line note on what it contributes to **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**.

Source	Cited work	What it contributes	Status
[238, 2026]	Recommendation on the Ethics of Artificial Intelligence	The official UNESCO page for the Recommendation on the Ethics of Artificial Intelligence, the first global standard-setting instrument on AI ethics, adopted in 2021 and applicable to all 194 member states. It outlines four core values, including human rights protection and environmental flourishing, and ten guiding principles such as proportionality, privacy, transparency, and fairness.	verified source-guide
[240, 2026]	The Right to Privacy in the Digital Age	The Office of the High Commissioner for Human Rights (OHCHR) hub page on the right to privacy in the digital age. It addresses how data-intensive technologies, particularly artificial intelligence, create risks for privacy, autonomy, and human dignity, and curates international standards, reports, and expert consultations.	verified source-guide
[241, 2026]	Modernised Convention 108	Official Council of Europe Convention 108+ source.	original source-guide
[274, 2026]	CAST Universal Design for Learning Guidelines version 3.0	The official CAST website for the Universal Design for Learning (UDL) Guidelines version 3.0, released in 2024. The framework offers research-based guidance for designing inclusive learning environments and is organized around three principles: Engagement (motivation and emotional support), Representation (accessible presentation of information), and Action and Expression (diverse means of participation and communication).	verified source-guide
[278, 2026]	Recommendation of the Council on Public Procurement	The OECD Recommendation of the Council on Public Procurement (OECD/LEGAL/0411), a legal instrument adopted by the OECD Council in 2015 on the proposal of the Public Governance Committee. It frames public procurement as a pillar of strategic governance and service delivery and sets out principles for governments to follow.	verified source-guide
[280, 2026]	NIST SP 800-61 Rev. 3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management	NIST SP 800-61 Rev. 3, published April 2025, integrates incident response guidance into broader cybersecurity risk management aligned with the NIST Cybersecurity Framework 2.0, superseding the 2012 Rev. 2. The publication addresses cyber threat information sharing, incident handling and management practices, and procedures for detecting, responding to, and recovering from security incidents.	verified source-guide

Source	Cited work	What it contributes	Status
[287, 2026]	Datasheets for Datasets	A 2018 arXiv paper proposing 'datasheets for datasets,' a standardized documentation framework for machine learning datasets modeled on electronic component datasheets. The authors argue the field lacks consistent dataset documentation, which creates risk in high-stakes applications, and propose that datasets be accompanied by documentation covering motivation, composition, collection process, recommended uses, and test results.	verified source-guide
[288, 2026]	Algorithmic Transparency Recording Standard Hub	A GOV.UK collection page serving as the hub for the UK Algorithmic Transparency Recording Standard (ATRS), maintained by the Government Digital Service. It provides a standardized template for documenting public-sector use of algorithmic tools, completion guidance, policy on scope and compliance, and a searchable repository of published transparency records.	verified source-guide
[295, 2026]	M-25-22: Driving Efficient Acquisition of Artificial Intelligence in Government	OMB Memorandum M-25-22 (April 3, 2025), Driving Efficient Acquisition of Artificial Intelligence in Government, issued under Executive Order 13960 and related directives. It provides guidance to federal agencies for acquiring effective and trustworthy AI in a timely, cost-effective manner, and rescinds and replaces earlier memorandum M-24-18.	verified source-guide
[012, 2026]	Counterintelligence Activities of Non-State Actors - Grey Dynamics	A Grey Dynamics analysis article (Rachel Brown, 2021) on how non-state actors conduct counterintelligence. It argues that although such groups lack the technical collection capabilities of states, they compensate through open-source and human-source methods and benefit defensively from compartmentalized, cell-based structures and ideological cohesion.	verified source-guide
[108, 2026]	Critical Thinking techniques	A Tradecraft Primer: Structured Analytic Techniques for Improving. Intelligence Analysis.	original source-guide
[029, 2026]	Agent Handling in Counterintelligence / PDF	A roughly 28-page Scribd document titled "Agent Handling in Counterintelligence" providing an educational overview of intelligence operations. It surveys the roles of case officers in managing sources, recruitment and training of agents, protective measures such as fronts and cutouts, agent classifications including unwitting sources, and counterintelligence methods for identifying foreign operatives and reducing security breaches.	verified source-guide context; do not use as primary analytic support
[297, 2026]	Intelligence Community Directive 203: Analytic Standards	Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products.	original source-guide
[298, 2026]	Intelligence Community Directives	Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations.	original source-guide

Where this sits. This module's overview is Section 33; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates

that govern this module.

33.3.4 Counterintelligence Fundamentals governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 33; [238, 2026].

33.3.5 Counterintelligence Fundamentals analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 22's governance-boundary section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **Counterintelligence and Source-Integrity Defense** for **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**. [238, 2026]; [240, 2026].

Curriculum topic spine: Source-vetting and insider-threat review using sample personnel records, **Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**, **Insider Threat Analysis: Source-vetting and insider-threat review using sample personnel records**. **Verified anchor cluster:** [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]; [Agency, 2009]; [Jr., 2007]; [Burkett, 2013].

Conceptual depth: defending institutions, sources, and judgments against deception, insider risk, foreign-intelligence targeting, and source contamination.

Method stack: threat awareness, source-descriptor audit, corroboration, anomaly review, red-team challenge, and protected disclosure paths.

Composability contract: identity, access, reporting, corroboration, caveats, and confidence are modeled independently so defensive review can happen without exposure.

Known failure modes: source compromise, deception acceptance, identity overconfidence, insider blind spots, and collapsing CI concerns into undifferentiated IT-security triage.

Defensive boundary: CI content supports defensive awareness, source protection, and analytic integrity; it does not provide surveillance or handling playbooks. Applied to **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**.

Anchor	Why it matters here
[Counterintelligence and Center, 2024]	Official strategy for defensive CI integration, foreign-intelligence threat awareness, strategic advantage protection, and future readiness. Checked as of 2026-05-21; role: curriculum_anchor.
[Archives and Administration, 1981]	Official legal anchor for intelligence authorities, rights-aware collection, analytic competition, oversight, and source-method protection. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026d]	Official sourcing directive for traceability, citations, source descriptors, and source summaries. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2015]	Official ODNI analytic tradecraft standards directive. Checked as of 2026-05-21; role: source_quality_anchor.
[Agency, 2009]	Official structured analytic techniques primer for bias checks, alternatives, and warning analysis. Checked as of 2026-05-21; role: curriculum_anchor.
[Jr., 2007]	Foundational analytic cognition source for bias, mental models, and structured reasoning. Checked as of 2026-06-06; role: curriculum_anchor.
[Burkett, 2013]	A CIA Studies in Intelligence analyst essay arguing that the traditional MICE recruitment-motivation model (Money, Ideology, Compromise, Ego) is better understood through Cialdini's influence principles reframed as RASCLS (Reciprocation, Authority, Scarcity, Commitment/Consistency, Liking, Social Proof), grounding the historical and conceptual lineage of HUMINT recruitment frameworks. Checked as of 2026-06-08; role: curriculum_anchor.

33.3.5.1 Counterintelligence Fundamentals evidence standard and citation floor: source families and discovery limits Official guidance supplies governance, safety, and legal constraints for the **Counterintelligence and Source-Integrity Defense** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [238, 2026]; [240, 2026].

33.3.6 Counterintelligence Fundamentals agentic boundary: assist, approve, block, and record

Evidence anchor. Section 33; [238, 2026].

AGEINT translation is bounded by the **Counterintelligence and Source-Integrity Defense** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**.

33.3.6.1 Counterintelligence Fundamentals permitted defensive utility: curriculum uses and safe outputs **Evidence anchor.** Section 33; [238, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**.

33.3.6.2 Counterintelligence Fundamentals excluded operational boundary: blocked actions and stop rules Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [238, 2026]; [240, 2026] and **Source-vetting and**

insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

33.3.7 Counterintelligence Fundamentals governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 33; [238, 2026].
Governance is practiced as a gate on the **Counterintelligence and Source-Integrity Defense** lane. Learners use the **Structured-Judgment Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**.

33.3.7.1 Counterintelligence Fundamentals governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [238, 2026]; [240, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Counterintelligence and Source-Integrity Defense** failure modes and the **Structured-Judgment Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

33.3.7.2 Counterintelligence Fundamentals evidence package handoff: appendices, records, and reuse

Evidence anchor. Section 33; [238, 2026].
Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Structured-Judgment Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**.

33.3.7.3 Counterintelligence Fundamentals current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**. [238, 2026]; [240, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_ncsc_counterintelligence_strategy` for **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**?	The National Counterintelligence Strategy; lane `counterintelligence_source_integrity`; checked 2026-05-21.	analytic note with hypotheses, evidence table, confidence, and dissent fields; Official strategy for defensive CI integration, foreign-intelligence threat awareness, strategic advantage protection, and future readiness.
What does the module inherit from `official_odni_eo_12333` for **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**?	Executive Order 12333: United States Intelligence Activities; lane `legal_oversight`; checked 2026-05-21.	analytic note with hypotheses, evidence table, confidence, and dissent fields; Official legal anchor for intelligence authorities, rights-aware collection, analytic competition, oversight, and source-method protection.
What does the module inherit from `official_odni_icd_206` for **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**?	Intelligence Community Directive 206: Sourcing Requirements for Disseminated Analytic Products; lane `analytic_tradecraft`; checked 2026-05-21.	analytic note with hypotheses, evidence table, confidence, and dissent fields; Official sourcing directive for traceability, citations, source descriptors, and source summaries.
What does the module inherit from `official_odni_icd_203` for **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**?	Intelligence Community Directive 203: Analytic Standards; lane `source_quality_spine`; checked 2026-05-21.	analytic note with hypotheses, evidence table, confidence, and dissent fields; Official ODNI analytic tradecraft standards directive.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 33; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

33.3.8 Counterintelligence Fundamentals assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 33; [238, 2026].

33.3.9 Counterintelligence Fundamentals assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 33; [238, 2026].

33.3.9.1 Counterintelligence Fundamentals capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records** and [238, 2026]; [240, 2026].

33.3.9.2 Counterintelligence Fundamentals instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records** and [238, 2026]; [240, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

33.3.9.3 Counterintelligence Fundamentals assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Source-vetting and insider-threat review using sample personnel records	Completed **analytic note with hypotheses, evidence table, confidence, and dissent fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records	Completed **analytic note with hypotheses, evidence table, confidence, and dissent fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Insider Threat Analysis: Source-vetting and insider-threat review using sample personnel records	Completed **analytic note with hypotheses, evidence table, confidence, and dissent fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

33.3.10 Counterintelligence Fundamentals refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [238, 2026]; [240, 2026] and **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**.

33.3.10.1 Counterintelligence Fundamentals refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**. The local signals begin with [238, 2026]; [240, 2026].

33.3.10.2 Counterintelligence Fundamentals claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**, and the source spine for these checks begins with [238, 2026]; [240, 2026].

33.3.11 Counterintelligence Fundamentals reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [238, 2026]; [240, 2026].

Triangulation anchors. In module 22's review-checklist section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records**. [238, 2026]; [240, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.

- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

33.3.12 Counterintelligence Fundamentals learning-path links: module map, overview, and curriculum atlas

Read this module in sequence with the curriculum orientation, its parent unit, and the adjacent modules so the evidence behind **Source-vetting and insider-threat review using sample personnel records; Offensive vs Defensive Counterintelligence: Source-vetting and insider-threat review using sample personnel records** carries forward intact. Source anchors for this module begin at [238, 2026]; [240, 2026].
Section 2, Section 32, Section 34

34 Counterintelligence Against Non-State Actors

34.0.1 Counterintelligence Against Non-State Actors figures and course links: visual evidence, source flow, and navigation

The module uses Figure 73 and Figure 70 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.

Navigation links: Section 2, Section 32, Section 33, Section 35.

This module teaches the **Counterintelligence and Source-Integrity Defense** lane through a bounded, source-backed coursebook chapter. [239, 2026]; [240, 2026].

34.1 Counterintelligence and Source-Integrity Defense frame for Counterintelligence Against Non-State Actors: source context, topic focus, and reader task

Evidence anchor. Section 34; [239, 2026].

34.1.1 Counterintelligence Against Non-State Actors orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 34; [239, 2026].

34.1.2 Counterintelligence Against Non-State Actors conceptual primer: source context, core model, and reader task

This chapter teaches counterintelligence as source-integrity defense: the class studies how institutions protect evidence, people, access, and judgment from deception and compromise. The chapter uses **Structured-Judgment Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**.

The central distinction is to separate defensive awareness from surveillance, handling, or operational security playbooks. Core topics include **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries; CI in Hybrid Threat Environments: Source-vetting and insider-threat review using sample personnel records**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.

Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [239, 2026]; [240, 2026].

Learners move from vocabulary and the **Structured-Judgment Lens** distinction through topic lessons on **Source-vetting and insider-threat review using sample personnel records** with evidence and misconception checks, then assemble an **analytic note with hypotheses, evidence table, confidence, and dissent fields** with safety and rights gates.

34.1.3 Counterintelligence Against Non-State Actors learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 34; [239, 2026].

- Connect **Source-vetting and insider-threat review using sample personnel records and Non-state actor indicator review with attribution caution and governance boundaries** to **Counterintelligence and Source-Integrity Defense** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build an **analytic note with hypotheses, evidence table, confidence, and dissent fields** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate defensive awareness from surveillance, handling, or operational security playbooks; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as source compromise, deception acceptance, identity overconfidence, insider blind spots, and collapsing CI concerns into undifferentiated IT-security triage, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: CI content supports defensive awareness, source protection, and analytic integrity; it does not provide surveillance or handling playbooks.

34.1.4 Counterintelligence Against Non-State Actors core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 34; [239, 2026].

Term	Working definition
Source integrity	confidence that evidence has not been distorted, laundered, or compromised
Compromise signal	a clue that access, identity, or source reliability needs review
Corroboration	independent support that reduces single-source vulnerability
Insider risk	risk created by trusted access combined with motive, pressure, or control failure
Protected disclosure	a safe channel for reporting concerns without exposing sensitive details
Source-vetting and insider-threat review using…	Key terms: vetting, insider, threat.
Non-state actor indicator review with…	Key terms: Non, state, actor.

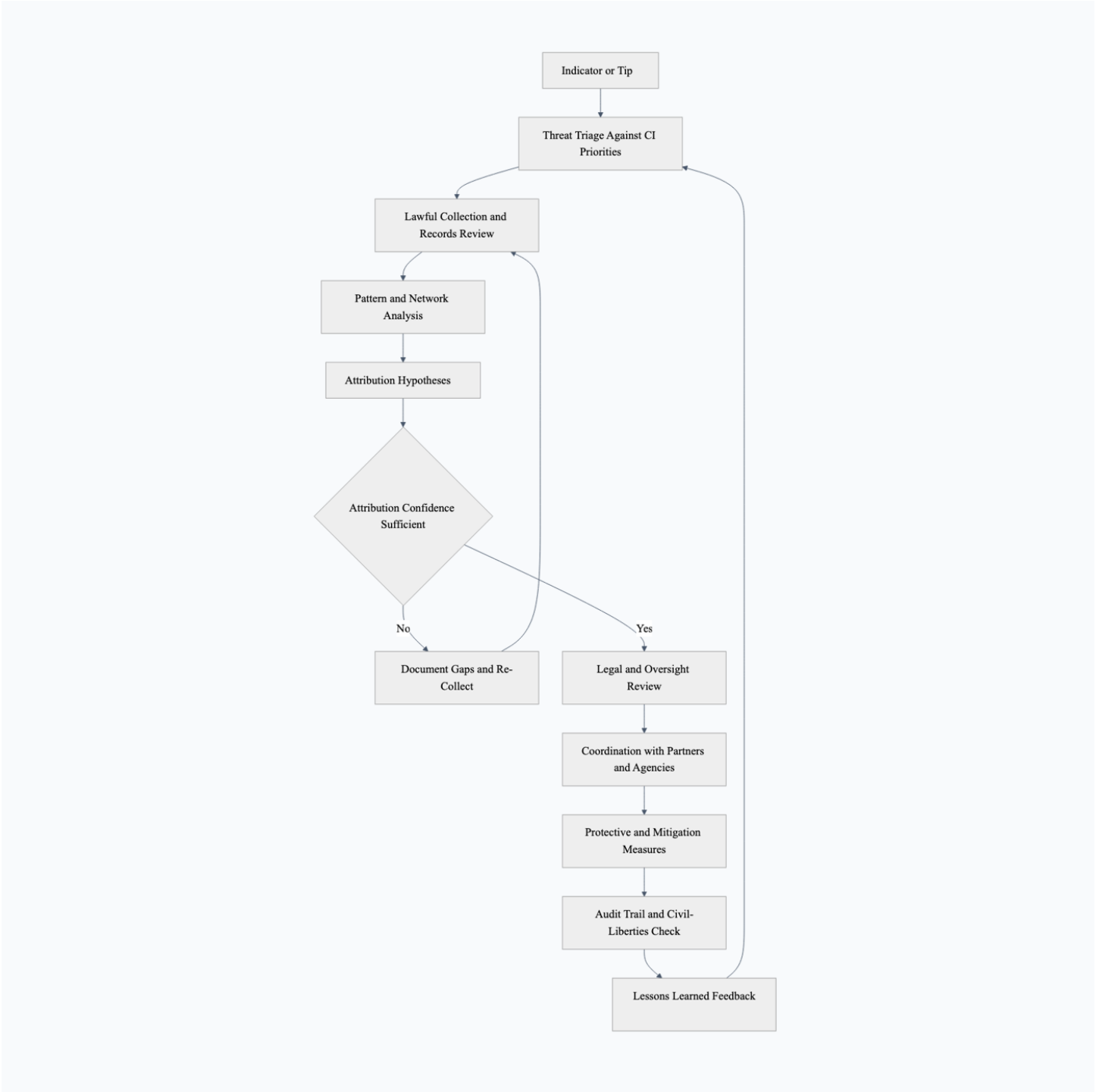


Figure 73: A governed counterintelligence loop showing how indicators against non-state actors move through lawful collection, attribution confidence checks, oversight review, and civil-liberties audit. The captioned view belongs to the counterintelligence / counterintelligence against non state actors section and should be read as a map of Indicator or Tip, Threat Triage Against CI Priorities, Lawful Collection and Records Review, and Pattern and Network Analysis, not as a capability score or live-task instruction.

34.2 Structured-Judgment Lens path for Counterintelligence Against Non-State Actors: lesson cluster, safe artifact, and review

Evidence anchor. Section 34; [239, 2026].

34.2.1 Counterintelligence Against Non-State Actors practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 34; [239, 2026].

34.2.2 Counterintelligence Against Non-State Actors topic lessons: source-backed concepts and transfer tasks

This module builds counterintelligence as source-integrity defense: the class studies how institutions protect evidence, people, access, and judgment from deception and compromise. The sequence opens with **Source-vetting and insider-threat review using sample personnel records**, **Non-state actor indicator review with attribution caution and governance boundaries**, **CI in Hybrid Threat Environments: Source-vetting and insider-threat review using sample personnel records** and applies the **Structured-Judgment Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 70; module overview Section 34; curriculum atlas Section 2.

Triangulation anchors. In module 23's topic-lessons section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

34.2.2.1 Lesson 1: Source-vetting and insider-threat review using sample personnel records

Concept. Source-vetting and insider-threat review using sample personnel records connects insider-threat review to access control, behavior indicators, and accountable escalation paths.

Why it matters. Source-vetting and insider-threat review using sample personnel records connects classroom vocabulary to Counterintelligence and Source-Integrity Defense practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Source-vetting and insider-threat review using sample personnel records rests on [012, 2026]. Its anchor reference records: A Grey Dynamics analysis article (Rachel Brown, 2021) on how non-state actors conduct counterintelligence. Use it for the claim that **Source-vetting and insider-threat review using sample personnel records** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. Read **Source-vetting and insider-threat review using sample personnel records** against the works cited for this row. [012, 2026] A Grey Dynamics analysis article (Rachel Brown, 2021) on how non-state actors conduct counterintelligence. It argues that although such groups lack the technical collection capabilities of states, they compensate through open-source and human-source methods and benefit defensively from compartmentalized, cell-based structures and ideological cohesion. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Source-vetting and insider-threat review using sample personnel records**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this deception-aware source review and defensive escalation topic. The artifact must record the vetting descriptor, the bounded claim about **Source-vetting and insider-threat review using**, the bias caveat, the uncertainty note, the unproven-allegation boundary, and the reviewer who adjudicates. Shape this subject work as a **source-integrity challenge memo** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Source-vetting and insider-threat review using sample personnel records**: that a clean vetting result certifies present trustworthiness rather than a point-in-time judgment that must be continuously re-examined.

Transfer task. Reuse the **Source-vetting and insider-threat review using sample personnel records** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

34.2.2.2 Lesson 2: Non-state actor indicator review with attribution caution and governance boundaries

Concept. Non-state actor indicator review with attribution caution and governance boundaries uses attribution indicators cautiously by separating technical similarity, context, confidence, and geopolitical inference.

Why it matters. Non-state actor indicator review matters in the **Counterintelligence and Source-Integrity Defense** lane because deception-aware source review and defensive escalation evidence must stay separate from judgment; source compromise is a common failure.

Source support. Non-state actor indicator review with attribution caution and governance boundaries rests on [033, 2026]. The lead source's own note reads: How seriously is the U.S. Use it for the claim that **Non-state actor indicator review with attribution caution and governance boundaries** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. For **Non-state actor indicator review**, work from the cited evidence behind this row. [033, 2026] How seriously is the U.S. Intelligence Community (IC) considering this challenge to U.S. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Non-state actor indicator review**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this deception-aware source review and defensive escalation topic. The artifact must name the actor descriptor, the bounded claim about **state actor indicator review with**, the attribution caveat, the uncertainty note, the non-targeting boundary, and the reviewer who approves the assessment. Shape **Non-state actor indicator review** work as a **source-integrity challenge memo** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that lacking a state sponsor places an actor outside the reach of governance, accountability, and applicable rules.

Transfer task. Transfer **Non-state actor indicator review** from this module to a second motif by preserving deception-aware source review and defensive escalation, replacing action with audit, and naming the blocked use.

34.2.2.3 Lesson 3: CI in Hybrid Threat Environments: Source-vetting and insider-threat review using sample personnel records

Concept. CI in Hybrid Threat Environments: Source-vetting and insider-threat review using sample personnel records connects insider-threat review to access control, behavior indicators, and accountable escalation paths.

Why it matters. CI in Hybrid Threat Environments matters in the **Counterintelligence and Source-Integrity Defense** lane because deception-aware source review and defensive escalation evidence must stay separate from judgment; source compromise is a common failure.

Source support. CI in Hybrid Threat Environments: Source-vetting and insider-threat review using sample personnel records rests on [109, 2026]. The most specific cited work observes: It analyzes how Russia, China, and Iran operate in the space between peace and war, describing Russia's emphasis on information measures, China's maritime and force approaches, and Iran's anti-access and proxy strategies. Use it for pinning down the scope of **CI in Hybrid Threat Environments: Source-vetting and insider-threat review using sample personnel records**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. For **CI in Hybrid Threat Environments**, reason from the sources cited in this row. [109, 2026] This is a peer-reviewed article in Connections: The Quarterly Journal (Vol. 21, No. 2, Spring 2022) by Peter Dobias and Kyle Christensen examining military competition below the threshold of armed conflict. It analyzes how Russia, China, and Iran operate in the space between peace and war, describing Russia's emphasis on information measures, China's maritime and force approaches, and Iran's anti-access and proxy strategies. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **CI in Hybrid Threat Environments**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this deception-aware source review and defensive escalation topic. The artifact must record the vetting descriptor, the bounded claim about **CI in Hybrid Threat Environments**, the bias caveat, the uncertainty note, the unproven-allegation boundary, and the reviewer who adjudicates. Shape **CI in Hybrid Threat Environments** work as a **source-integrity challenge memo** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **CI in Hybrid Threat Environments**: that a clean vetting result certifies present trustworthiness rather than a point-in-time judgment that must be continuously re-examined.

Transfer task. Reuse the **CI in Hybrid Threat Environments** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

34.2.2.4 Lesson 4: Attribution Problems in State CI: Source-vetting and insider-threat review using sample personnel records

Concept. Attribution Problems in State CI: Source-vetting and insider-threat review using sample personnel records uses attribution indicators cautiously by separating technical similarity, context, confidence, and geopolitical inference.

Why it matters. Attribution Problems in State CI connects classroom vocabulary to Counterintelligence and Source-Integrity Defense practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Attribution Problems in State CI: Source-vetting and insider-threat review using sample personnel records rests on [033, 2026]. The lead source's own note reads: How seriously is the U.S. Use it for the claim that **Attribution Problems in State CI: Source-vetting and insider-threat review using sample personnel records** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. For **Attribution Problems in State CI**, reason from the sources cited in this row. [033, 2026] How seriously is the U.S. Intelligence Community (IC) considering this challenge to U.S. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Attribution Problems in State CI**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this deception-aware source review and defensive escalation topic. The artifact must record the vetting descriptor, the bounded claim about **Attribution Problems in State CI**, the bias caveat, the uncertainty note, the unproven-allegation boundary, and the reviewer who adjudicates. Shape **Attribution Problems in State CI** work as a **source-integrity challenge memo** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Attribution Problems in State CI**: that a clean vetting result certifies present trustworthiness rather than a point-in-time judgment that must be continuously re-examined.

Transfer task. Transfer **Attribution Problems in State CI** from this module to a second motif by preserving deception-aware source review and defensive escalation, replacing action with audit, and naming the blocked use.

34.2.2.5 Lesson 5: Corporate Counterintelligence and Trade Secret: Source-vetting and insider-threat review using sample personnel records

Concept. Corporate Counterintelligence and Trade Secret: Source-vetting and insider-threat review using sample personnel records frames counterintelligence as source-vetting, anomaly review, and institutional protection—not operational entrapment.

Why it matters. Corporate Counterintelligence and Trade Secret connects classroom vocabulary to Counterintelligence and Source-Integrity Defense practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Corporate Counterintelligence and Trade Secret: Source-vetting and insider-threat review using sample personnel records rests on [307, 2026], [305, 2026], and [304, 2026]. The lead source's own note reads: NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Use them for pinning down the scope of **Corporate Counterintelligence and Trade Secret: Source-vetting and insider-threat review using sample personnel records**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. For **Corporate Counterintelligence and Trade Secret**, reason from the sources cited in this row. [307, 2026] Official CISA Industrial Control Systems recommended practices page for defensive ICS/OT safety, resilience, and incident-preparation guidance. [305, 2026] Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Corporate Counterintelligence and Trade Secret**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this deception-aware source review and defensive escalation topic. The artifact must record the vetting descriptor, the bounded claim about **Corporate Counterintelligence and Trade Secret**, the bias caveat, the uncertainty note, the unproven-allegation boundary, and the reviewer who adjudicates. Shape **Corporate Counterintelligence and Trade Secret** work as a **source-integrity challenge memo** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Corporate Counterintelligence and Trade Secret**: that a clean vetting result certifies present trustworthiness rather than a point-in-time judgment that must be continuously re-examined.

Transfer task. Apply this module's safe boundary for **Corporate Counterintelligence and Trade Secret** to another artifact while keeping deception-aware source review and defensive escalation and reviewer ownership explicit.

34.2.3 Counterintelligence Against Non-State Actors worked safe example: synthetic inputs, evidence, and review

Worked example: a sample research lab reviews a synthetic source-quality anomaly after a disputed report. [239, 2026]; [240, 2026].

Triangulation anchors. In module 23's worked-example section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **source-integrity defense**. Learners use a **source-integrity challenge memo** and keep this boundary visible: No surveillance, cover construction, handling, elicitation, or operational security playbooks.

Frame. The classroom question centers on **Source-vetting and insider-threat review using sample personnel records**. Excluded actions stay explicit, and the **Structured-Judgment Lens** planning question is: Which assumptions, alternatives, confidence statements, and source limits must stay visible for review?

Inputs. For the **Source-vetting and insider-threat review using sample personnel records** scenario, use toy access logs, public policy excerpts, synthetic source notes, and a reviewer escalation path. The Structured-Judgment Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Source-vetting and insider-threat review using sample personnel records**, students separate identity from access, list anomaly hypotheses, seek corroboration, and route sensitive concerns to review. Pause whenever an inference about Source-vetting and insider-threat review using sample personnel records appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Source-vetting and insider-threat review using sample personnel records** classroom scenario; unit artifact = source-integrity challenge memo; evidence = allowed inputs; method = deception-aware source review and defensive escalation; output = a source-integrity memo with competing explanations, confidence, protected-disclosure note, and next-review owner; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Source-vetting and insider-threat review using sample personnel records** as "Structured-Judgment Lens confirms it" is not enough. The revision ties the claim to deception-aware source review and defensive escalation, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Source-vetting and insider-threat review using sample personnel records** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

34.2.4 Counterintelligence Against Non-State Actors practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Structured-Judgment Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**.

Triangulation anchors. In module 23's practice-sequence section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Source-vetting and insider-threat review using sample personnel records, Non-state actor indicator review with attribution caution and governance boundaries, CI in Hybrid Threat Environments: Source-vetting and insider-threat review using sample personnel records; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Counterintelligence and Source-Integrity Defense** lane.
2. Frame	Answer the lens question: Which assumptions, alternatives, confidence statements, and source limits must stay visible for review?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Source-vetting and insider-threat review using sample personnel records: analytic note with hypotheses, evidence table, confidence, and dissent fields.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the source-integrity challenge memo fields for Source-vetting and insider-threat review using sample personnel records.	Unit profile note.	Evidence artifacts include anomaly hypothesis table, corroboration note.
4. Challenge	Test the misconception that a clean vetting result certifies present trustworthiness rather than a point-in-time judgment that must be continuously re-examined.	Failure-mode note.	The artifact applies the key distinction: separate defensive awareness from surveillance, handling, or operational security playbooks.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

34.2.4.1 Counterintelligence Against Non-State Actors instructor notes: source reasoning, review points, and studio focus

Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**. [239, 2026]; [240, 2026].

34.2.4.2 Counterintelligence Against Non-State Actors extension exercise: peer validation and refresh trigger review

Evidence anchor. Section 34; [239, 2026].

Have learners swap artifacts and apply the **Structured-Judgment Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**.

34.2.5 Counterintelligence Against Non-State Actors knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 34; [239, 2026].

1. Explain how **Source-vetting and insider-threat review using sample personnel records** is defined here; name the source descriptor that supports the definition.
2. Contrast **Source-vetting and insider-threat review using sample personnel records** with **Non-state actor indicator review with attribution caution and governance boundaries** using the **Structured-Judgment Lens** artifact fields.

3. Identify one failure mode from the **Counterintelligence and Source-Integrity Defense** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which explanation preserves uncertainty without ignoring a possible compromise signal?
5. Correct this misconception: that a clean vetting result certifies present trustworthiness rather than a point-in-time judgment that must be continuously re-examined.

34.2.5.1 Counterintelligence Against Non-State Actors answer quality rubric: source evidence, uncertainty, and safe transfer
Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Source-vetting and insider-threat review using sample personnel records** without source evidence, uncertainty, or a safe transfer task.

34.3 Counterintelligence Against Non-State Actors assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 34; [239, 2026].

34.3.1 Counterintelligence Against Non-State Actors evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 34; [239, 2026].

34.3.2 Counterintelligence Against Non-State Actors transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 34; [239, 2026].

34.3.2.1 Counterintelligence Against Non-State Actors lineage and source tradition: profile, concepts, and first anchors This sits in the **Counterintelligence and Source-Integrity Defense** lineage: defending institutions, sources, and judgments against deception, insider risk, foreign-intelligence targeting, and source contamination. [239, 2026]; [240, 2026].

34.3.2.2 Counterintelligence Against Non-State Actors working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 34; [239, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**, with provenance and reviewability throughout.

34.3.2.3 Counterintelligence Against Non-State Actors knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [239, 2026]; [240, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

34.3.2.4 Counterintelligence Against Non-State Actors transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 34; [239, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**.
- **Evidence contract:** keep the **Counterintelligence and Source-Integrity Defense** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

34.3.2.5 Counterintelligence Against Non-State Actors profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 34; [239, 2026].

The matched profile emphasizes defending institutions, sources, and judgments against deception, insider risk, foreign-intelligence targeting, and source contamination. The method stack is threat awareness, source-descriptor audit, corroboration, anomaly review, red-team challenge, and protected disclosure paths; the local topic cluster is **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**.

34.3.3 Counterintelligence Against Non-State Actors evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 34; [239, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Counterintelligence and Source-Integrity Defense** profile tells reviewers what evidence is strong enough for the module artifact built around **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**.

34.3.3.1 Counterintelligence Against Non-State Actors guide source spine: inherited keys and local citation roles Primary guide citations: [239, 2026]; [240, 2026]; [241, 2026]; [279, 2026]; [282, 2026]; [284, 2026]; [289, 2026]; [291, 2026]; [296, 2026]; [012, 2026]; [033, 2026]; [109, 2026]; [307, 2026]; [305, 2026]; [304, 2026].

34.3.3.2 Counterintelligence Against Non-State Actors verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [239, 2026]; [240, 2026].

Tier	What counts	How it is used
Source guide	[239, 2026]; [240, 2026]; [241, 2026]; [279, 2026]; [282, 2026]; [284, 2026]; [289, 2026]; [291, 2026]; [296, 2026]; [012, 2026]; [033, 2026]; [109, 2026]; [307, 2026]; [305, 2026]; [304, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 23's source-canon section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries** and [239, 2026]; [240, 2026], but only directly verified source URLs are encoded as citations.

34.3.3.3 Counterintelligence Against Non-State Actors intelligence practice lens: evidence artifact and safety check Practice lens: **Structured-Judgment Lens** for **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**. [239, 2026]; [240, 2026].

Planning question: Which assumptions, alternatives, confidence statements, and source limits must stay visible for review?

Evidence artifact: analytic note with hypotheses, evidence table, confidence, and dissent fields.

Validation rule: separate raw reporting, inference, judgment, and recommendation before synthesis. Applied to **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**.

Handoff contract: handoff preserves alternatives, uncertainty, caveats, and revision history for downstream modules.

Safety check: avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence.

34.3.3.4 Counterintelligence Against Non-State Actors runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 34; [239, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	23.99	23.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Counterintelligence Against Non-State Actors to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Bounded autonomy, procurement, incident-response, and assurance studio	23.101	23.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Counterintelligence Against Non-State Actors	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Model-card, recoverability, retention, and learner-support evidence package	23.102	23.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Counterintelligence Against Non-State Actors	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-vetting and insider-threat review using sample personnel records	23.1	23.1 source title transformed into safe curriculum treatment; original: CI Against Terrorist and Criminal Intelligence Networks	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Non-state actor indicator review with attribution caution and governance boundaries	23.2	23.2 source title transformed into safe curriculum treatment; original: The Counterintelligence Threat from Non-State Actors	AI/Data Accountability Lens	AI/data impact card with authority, provenance, model version, impact score, register status, human owner, and review cadence	reject automated adverse action, hidden surveillance expansion, unowned outputs, unreviewed model drift, and opaque downstream reuse
Source-vetting and insider-threat review using sample personnel records	23.3	23.3 source title transformed into safe curriculum treatment; original: CI in Hybrid Threat Environments	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Source-vetting and insider-threat review using sample personnel records	23.4	23.4 source title transformed into safe curriculum treatment; original: Attribution Problems in Non-State CI Operations	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Source-vetting and insider-threat review using sample personnel records	23.5	23.5 source title transformed into safe curriculum treatment; original: Corporate Counterintelligence and Trade Secret Protection	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

34.3.3.5 Counterintelligence Against Non-State Actors reusable subsection contract: topic rows, artifacts, and safety duties **Evidence anchor.** Section 34; [239, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Source-vetting and insider-threat review using sample personnel records	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Non-state actor indicator review with attribution caution and governance boundaries	AI/Data Accountability Lens	AI/data impact card with authority, provenance, model version, impact score, register status, human owner, and review cadence	reject automated adverse action, hidden surveillance expansion, unowned outputs, unreviewed model drift, and opaque downstream reuse
CI in Hybrid Threat Environments: Source-vetting and insider-threat review using sample personnel records	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Attribution Problems in State CI: Source-vetting and insider-threat review using sample personnel records	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Corporate Counterintelligence and Trade Secret: Source-vetting and insider-threat review using sample personnel records	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

34.3.3.6 Counterintelligence Against Non-State Actors annotated source ledger: real titles and local contribution Each source cited by this **Counterintelligence and Source-Integrity Defense** module is paired below with its real title and a one-line note on what it contributes to **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**.

Source	Cited work	What it contributes	Status
[239, 2026]	Digital Space and Human Rights	Official OHCHR digital rights portal.	original source-guide

Source	Cited work	What it contributes	Status
[240, 2026]	The Right to Privacy in the Digital Age	The Office of the High Commissioner for Human Rights (OHCHR) hub page on the right to privacy in the digital age. It addresses how data-intensive technologies, particularly artificial intelligence, create risks for privacy, autonomy, and human dignity, and curates international standards, reports, and expert consultations.	verified source-guide
[241, 2026]	Modernised Convention 108	Official Council of Europe Convention 108+ source.	original source-guide
[279, 2026]	Open Contracting Data Standard	The documentation homepage for the Open Contracting Data Standard, version 1.1.5, maintained by the Open Contracting Partnership to support disclosure of government contracting data across the procurement lifecycle. It provides a common data model spanning planning, tender, award, contract, and implementation stages, along with a primer, implementation guidance, technical schemas, and validation tooling.	verified source-guide
[282, 2026]	AI Research: Security and Resilience	A NIST page on AI research focused on security and resilience, framing these as core characteristics of trustworthy AI under the NIST AI Risk Management Framework.	verified source-guide
[284, 2026]	Verifiable Credential Data Integrity 1.0	The W3C Recommendation for Verifiable Credential Data Integrity 1.0, published May 2025, defining mechanisms for ensuring the authenticity and integrity of verifiable credentials using cryptographic proofs. It specifies a process of data transformation, hashing, and proof generation, and a corresponding verification procedure, along with a proof data model containing properties such as type, verification method, purpose, and proof value.	verified source-guide
[289, 2026]	Guidance for Organisations Using the Algorithmic Transparency Recording Standard	This is a GOV.UK guidance page published by the Government Digital Service that instructs public sector organizations on completing the Algorithmic Transparency Recording Standard (ATRS) template and publishing their records to the GOV.UK repository. It applies both to central government bodies required to publish under mandatory policy and to other public sector bodies doing so voluntarily.	verified source-guide
[291, 2026]	Revised 508 Standards and 255 Guidelines	Official documentation from the U.S. Access Board on the Revised 508 Standards and 255 Guidelines for information and communication technology accessibility. It establishes mandatory accessibility requirements for federal agencies and voluntary guidelines for telecommunications manufacturers, covering hardware, software, websites, electronic documents, and support services.	verified source-guide

Source	Cited work	What it contributes	Status
[296, 2026]	Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile	NIST AI 600-1, the Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, a cross-sectoral companion resource to the NIST AI RMF 1.0 issued pursuant to Executive Order 14110. It identifies risks that are unique to or amplified by generative AI and organizes suggested actions for managing those risks, mapped to the AI RMF functions.	verified source-guide
[012, 2026]	Counterintelligence Activities of Non-State Actors - Grey Dynamics	A Grey Dynamics analysis article (Rachel Brown, 2021) on how non-state actors conduct counterintelligence. It argues that although such groups lack the technical collection capabilities of states, they compensate through open-source and human-source methods and benefit defensively from compartmentalized, cell-based structures and ideological cohesion.	verified source-guide
[033, 2026]	The Counterintelligence Threat from Non-State Actors	How seriously is the U.S. Intelligence Community (IC) considering this challenge to U.S.	original source-guide context; do not use as primary analytic support
[109, 2026]	The 'Grey Zone' and Hybrid Activities	This is a peer-reviewed article in Connections: The Quarterly Journal (Vol. 21, No. 2, Spring 2022) by Peter Dobias and Kyle Christensen examining military competition below the threshold of armed conflict. It analyzes how Russia, China, and Iran operate in the space between peace and war, describing Russia's emphasis on information measures, China's maritime and force approaches, and Iran's anti-access and proxy strategies.	verified source-guide
[307, 2026]	ICS Recommended Practices	Official CISA Industrial Control Systems recommended practices page for defensive ICS/OT safety, resilience, and incident-preparation guidance.	original source-guide
[305, 2026]	DevSecOps	Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support.	original source-guide
[304, 2026]	Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities	NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences.	verified source-guide

Where this sits. This module's overview is Section 34; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

34.3.4 Counterintelligence Against Non-State Actors governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 34; [239, 2026].

34.3.5 Counterintelligence Against Non-State Actors analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 23's governance-boundary section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **Counterintelligence and Source-Integrity Defense** for **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**. [239, 2026]; [240, 2026].

Curriculum topic spine: Source-vetting and insider-threat review using sample personnel records, **Non-state actor indicator review with attribution caution and governance boundaries**, **CI in Hybrid Threat Environments: Source-vetting and insider-threat review using sample personnel records**. **Verified anchor cluster:** [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]; [Agency, 2009]; [Jr., 2007]; [Burkett, 2013].

Conceptual depth: defending institutions, sources, and judgments against deception, insider risk, foreign-intelligence targeting, and source contamination.

Method stack: threat awareness, source-descriptor audit, corroboration, anomaly review, red-team challenge, and protected disclosure paths.

Composability contract: identity, access, reporting, corroboration, caveats, and confidence are modeled independently so defensive review can happen without exposure.

Known failure modes: source compromise, deception acceptance, identity overconfidence, insider blind spots, and collapsing CI concerns into undifferentiated IT-security triage.

Defensive boundary: CI content supports defensive awareness, source protection, and analytic integrity; it does not provide surveillance or handling playbooks. Applied to **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**.

Anchor	Why it matters here
[Counterintelligence and Center, 2024]	Official strategy for defensive CI integration, foreign-intelligence threat awareness, strategic advantage protection, and future readiness. Checked as of 2026-05-21; role: curriculum_anchor.
[Archives and Administration, 1981]	Official legal anchor for intelligence authorities, rights-aware collection, analytic competition, oversight, and source-method protection. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026d]	Official sourcing directive for traceability, citations, source descriptors, and source summaries. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2015]	Official ODNI analytic tradecraft standards directive. Checked as of 2026-05-21; role: source_quality_anchor.
[Agency, 2009]	Official structured analytic techniques primer for bias checks, alternatives, and warning analysis. Checked as of 2026-05-21; role: curriculum_anchor.
[Jr., 2007]	Foundational analytic cognition source for bias, mental models, and structured reasoning. Checked as of 2026-06-06; role: curriculum_anchor.
[Burkett, 2013]	A CIA Studies in Intelligence analyst essay arguing that the traditional MICE recruitment-motivation model (Money, Ideology, Compromise, Ego) is better understood through Cialdini's influence principles reframed as RASCLS (Reciprocation, Authority, Scarcity, Commitment/Consistency, Liking, Social Proof), grounding the historical and conceptual lineage of HUMINT recruitment frameworks. Checked as of 2026-06-08; role: curriculum_anchor.

34.3.5.1 Counterintelligence Against Non-State Actors evidence standard and citation floor: source families and discovery limits Official guidance supplies governance, safety, and legal constraints for the **Counterintelligence and Source-Integrity Defense** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [239, 2026]; [240, 2026].

34.3.6 Counterintelligence Against Non-State Actors agentic boundary: assist, approve, block, and record

Evidence anchor. Section 34; [239, 2026].

AGEINT translation is bounded by the **Counterintelligence and Source-Integrity Defense** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**.

34.3.6.1 Counterintelligence Against Non-State Actors permitted defensive utility: curriculum uses and safe outputs Evidence anchor. Section 34; [239, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**.

34.3.6.2 Counterintelligence Against Non-State Actors excluded operational boundary: blocked actions and stop rules Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [239, 2026]; [240, 2026] and **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

34.3.7 Counterintelligence Against Non-State Actors governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 34; [239, 2026].
Governance is practiced as a gate on the **Counterintelligence and Source-Integrity Defense** lane. Learners use the **Structured-Judgment Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**.

34.3.7.1 Counterintelligence Against Non-State Actors governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [239, 2026]; [240, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Counterintelligence and Source-Integrity Defense** failure modes and the **Structured-Judgment Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

34.3.7.2 Counterintelligence Against Non-State Actors evidence package handoff: appendices, records, and reuse

Evidence anchor. Section 34; [239, 2026].
Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Structured-Judgment Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**.

34.3.7.3 Counterintelligence Against Non-State Actors current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**. [239, 2026]; [240, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_ncsc_counterintelligence_strategy` for **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**?	The National Counterintelligence Strategy; lane `counterintelligence_source_integrity`; checked 2026-05-21.	analytic note with hypotheses, evidence table, confidence, and dissent fields; Official strategy for defensive CI integration, foreign-intelligence threat awareness, strategic advantage protection, and future readiness.
What does the module inherit from `official_odni_eo_12333` for **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**?	Executive Order 12333: United States Intelligence Activities; lane `legal_oversight`; checked 2026-05-21.	analytic note with hypotheses, evidence table, confidence, and dissent fields; Official legal anchor for intelligence authorities, rights-aware collection, analytic competition, oversight, and source-method protection.
What does the module inherit from `official_odni_icd_206` for **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**?	Intelligence Community Directive 206: Sourcing Requirements for Disseminated Analytic Products; lane `analytic_tradecraft`; checked 2026-05-21.	analytic note with hypotheses, evidence table, confidence, and dissent fields; Official sourcing directive for traceability, citations, source descriptors, and source summaries.
What does the module inherit from `official_odni_icd_203` for **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**?	Intelligence Community Directive 203: Analytic Standards; lane `source_quality_spine`; checked 2026-05-21.	analytic note with hypotheses, evidence table, confidence, and dissent fields; Official ODNI analytic tradecraft standards directive.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 34; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

34.3.8 Counterintelligence Against Non-State Actors assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 34; [239, 2026].

34.3.9 Counterintelligence Against Non-State Actors assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 34; [239, 2026].

34.3.9.1 Counterintelligence Against Non-State Actors capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**.
Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries** and [239, 2026]; [240, 2026].

34.3.9.2 Counterintelligence Against Non-State Actors instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries** and [239, 2026]; [240, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

34.3.9.3 Counterintelligence Against Non-State Actors assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Source-vetting and insider-threat review using sample personnel records	Completed **analytic note with hypotheses, evidence table, confidence, and dissent fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Non-state actor indicator review with attribution caution and governance boundaries	Completed **analytic note with hypotheses, evidence table, confidence, and dissent fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
CI in Hybrid Threat Environments: Source-vetting and insider-threat review using sample personnel records	Completed **analytic note with hypotheses, evidence table, confidence, and dissent fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

34.3.10 Counterintelligence Against Non-State Actors refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [239, 2026]; [240, 2026] and **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**.

34.3.10.1 Counterintelligence Against Non-State Actors refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**. The local signals begin with [239, 2026]; [240, 2026].

34.3.10.2 Counterintelligence Against Non-State Actors claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**, and the source spine for these checks begins with [239, 2026]; [240, 2026].

34.3.11 Counterintelligence Against Non-State Actors reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [239, 2026]; [240, 2026].
Triangulation anchors. In module 23's review-checklist section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries**. [239, 2026]; [240, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.

- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

34.3.12 Counterintelligence Against Non-State Actors learning-path links: module map, overview, and curriculum atlas

Read this module in sequence with the curriculum orientation, its parent unit, and the adjacent modules so the evidence behind **Source-vetting and insider-threat review using sample personnel records; Non-state actor indicator review with attribution caution and governance boundaries** carries forward intact. Source anchors for this module begin at [239, 2026]; [240, 2026].

Section 2, Section 32, Section 33, Section 35

35 GRAY ZONE, HYBRID WARFARE, AND NON-STATE ACTORS

35.1 GRAY ZONE, HYBRID WARFARE, AND NON-STATE ACTORS learning spine and source route: unit purpose, module order, and evidence handoff

Evidence anchor. Section 35; [239, 2026].

35.1.1 hybrid-threat governance discipline spine: domain question and learning focus

Evidence anchor. Section 35; [239, 2026].
This unit teaches **hybrid-threat governance**. Gray-zone lessons analyze ambiguous coercion, proxy relationships, resilience choices, and policy thresholds without operationalizing response.

35.1.2 hybrid-threat governance source-use contract: citation roles and evidence limits

Evidence anchor. Section 35; [239, 2026].
Use official and alliance anchors for threshold language, information threats, and resilience governance.

35.1.3 hybrid-threat governance practice artifact: recurring packet and retained evidence

Evidence anchor. Section 35; [239, 2026].
The recurring practice artifact is a **ambiguous-threshold indicator matrix** that draws on threshold indicator, attribution caveat, proxy-pattern note, and policy review field. The unit keeps its learning spine explicit. Learners distinguish observable indicators from sponsorship claims and state the review needed before action.

35.1.4 hybrid-threat governance safety boundary: accountable, synthetic, and evidence-bounded limits

No live targeting, covert action, retaliation planning, or attribution certainty beyond evidence.
This unit introduces the part's governing question, evidence artifacts, source-support spine, and capstone thread before the individual modules begin. [239, 2026]; [247, 2026].
Learners carry one unit capstone thread through the part: define an accountable intelligence question, bind it to source-quality constraints, produce a reviewable artifact, test the artifact against failure modes, and hand it off with enough context for another analyst or instructor to audit. The capstone remains public, synthetic, or owned-lab throughout; its first source anchors are [239, 2026]; [247, 2026].
This unit's deliverables are a source-canon card, claim/evidence ledger, safe-practice lab packet, failure-mode note, instructor rubric, and debrief memo. The full source-lane and evidence-package ledgers appear in the orientation and appendices; this unit introduction keeps only the learner-facing spine for [239, 2026]; [247, 2026].
This unit's safety gates are scope authorization, rights review, data provenance, tool allowlisting, human oversight, rollback, and evidence-bounded output. A missing gate turns the activity into a tabletop, audit, or written governance exercise until the gate is restored against [239, 2026]; [247, 2026].
Capstone thread:

Phase	Artifact	Review gate
Question	accountable learning question and excluded-action list	instructor confirms scope, allowed data, and rights impact
Source canon	source-lane map with guide citations, verified anchors, and refresh dates	citation keys resolve and source identity lock remains stable
Evidence ledger	claim, evidence, uncertainty, confidence, and reviewer register	every material claim has a source, caveat, and owner
Safe lab	synthetic or public dataset packet, tool allowlist, and stop conditions	no live target, private data, external action, or unsafe cyber-physical step
Assurance	evaluation rubric, failure-mode drill, rights map, and remediation note	human reviewer signs off before presentation or reuse
Debrief	capstone memo with lessons, residual risk, refresh triggers, and handoff owner	all unresolved questions and future approvals are explicit

Research lane: Counterintelligence and Source-Integrity Defense. Core anchors: [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]. Conceptual focus: defending institutions, sources, and judgments against deception, insider risk, foreign-intelligence targeting, and source contamination. Composability contract: identity, access, reporting, corroboration, caveats, and confidence are modeled independently so defensive review can happen without exposure. **Practice lens:** Dissemination-and-Marking Control Lens; Which audience, release authority, marking vocabulary, records duty, and feedback loop governs this intelligence artifact? [239, 2026]; [247, 2026].

35.1.5 GRAY ZONE, HYBRID WARFARE, AND NON-STATE ACTORS visual navigation and module map: evidence flow, order, and safety cues

The unit uses Figure 74 and Figure 75 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 34, Section 36.

35.1.6 GRAY ZONE, HYBRID WARFARE, AND NON-STATE ACTORS module roster and source-lane inventory: citations, lanes, and learner route

Module	Section reference	Source spine
Gray Zone Warfare	Section 36	[239, 2026]; [247, 2026]; [249, 2026]; [275, 2026]; [276, 2026]; [283, 2026]; [286, 2026]; [293, 2026]; [295, 2026]; [109, 2026]; [110, 2026]; [111, 2026]; [308, 2026]; [311, 2026].
Non-State Actor Intelligence	Section 37	[238, 2026]; [247, 2026]; [249, 2026]; [273, 2026]; [274, 2026]; [275, 2026]; [286, 2026]; [287, 2026]; [292, 2026]; [012, 2026]; [033, 2026]; [308, 2026]; [311, 2026]; [309, 2026]; [310, 2026]; [300, 2026].

Module	Section reference	Source spine
Irregular Warfare and Special Operations	Section 38	[239, 2026]; [249, 2026]; [266, 2026]; [276, 2026]; [277, 2026]; [284, 2026]; [288, 2026]; [289, 2026]; [293, 2026]; [112, 2026]; [113, 2026]; [114, 2026]; [115, 2026]; [116, 2026]; [117, 2026]; [118, 2026]; [119, 2026]; [120, 2026]; [308, 2026]; [311, 2026].

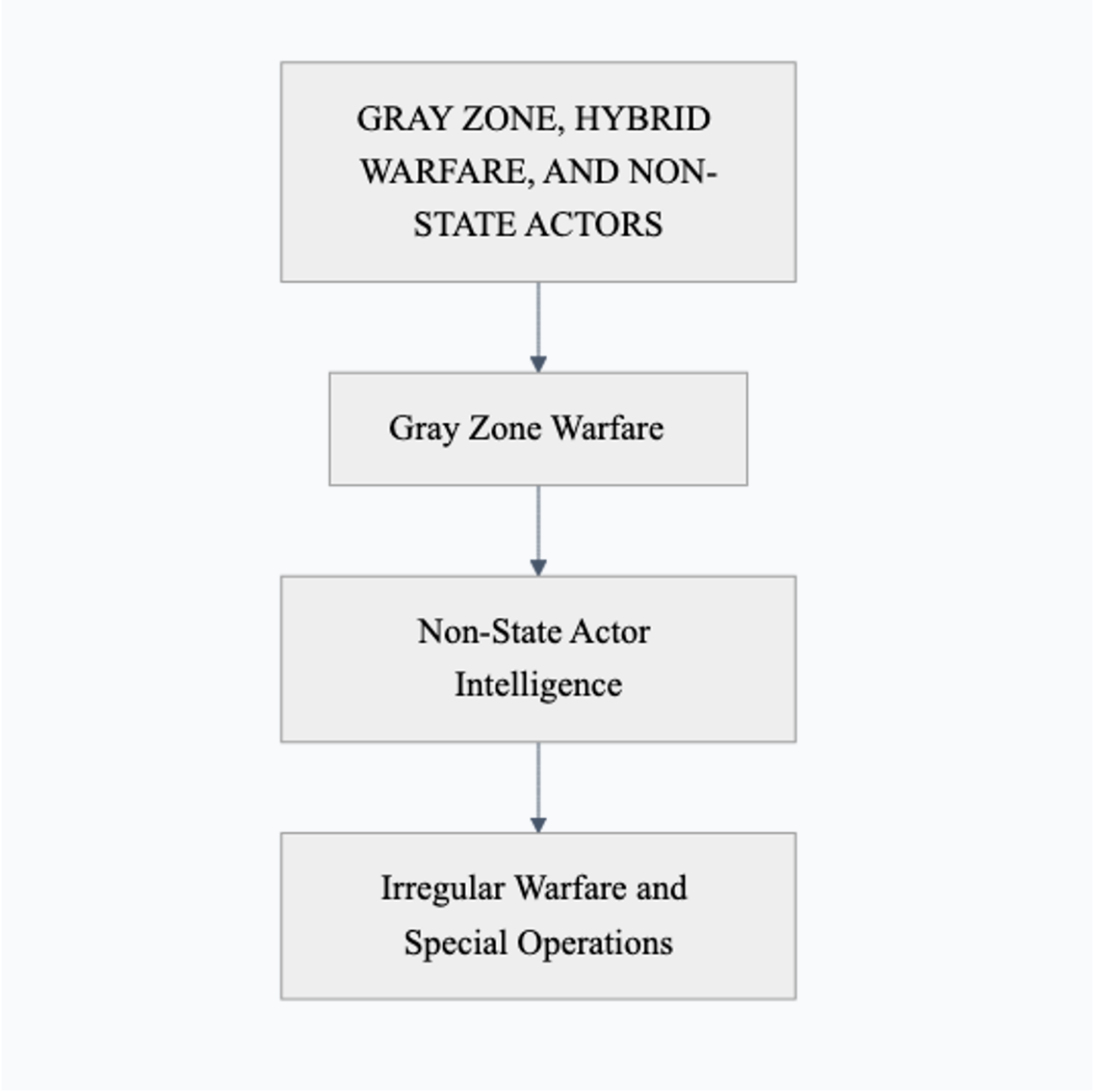


Figure 74: The unit module map traces the part's chapters as a linear reading sequence. In the gray zone hybrid warfare and non state actors section, it lets readers compare 3 module nodes in the unit's ordered, source-backed reading sequence from its first module to its last so the visual functions as a traceable course aid rather than an unscoped assertion.

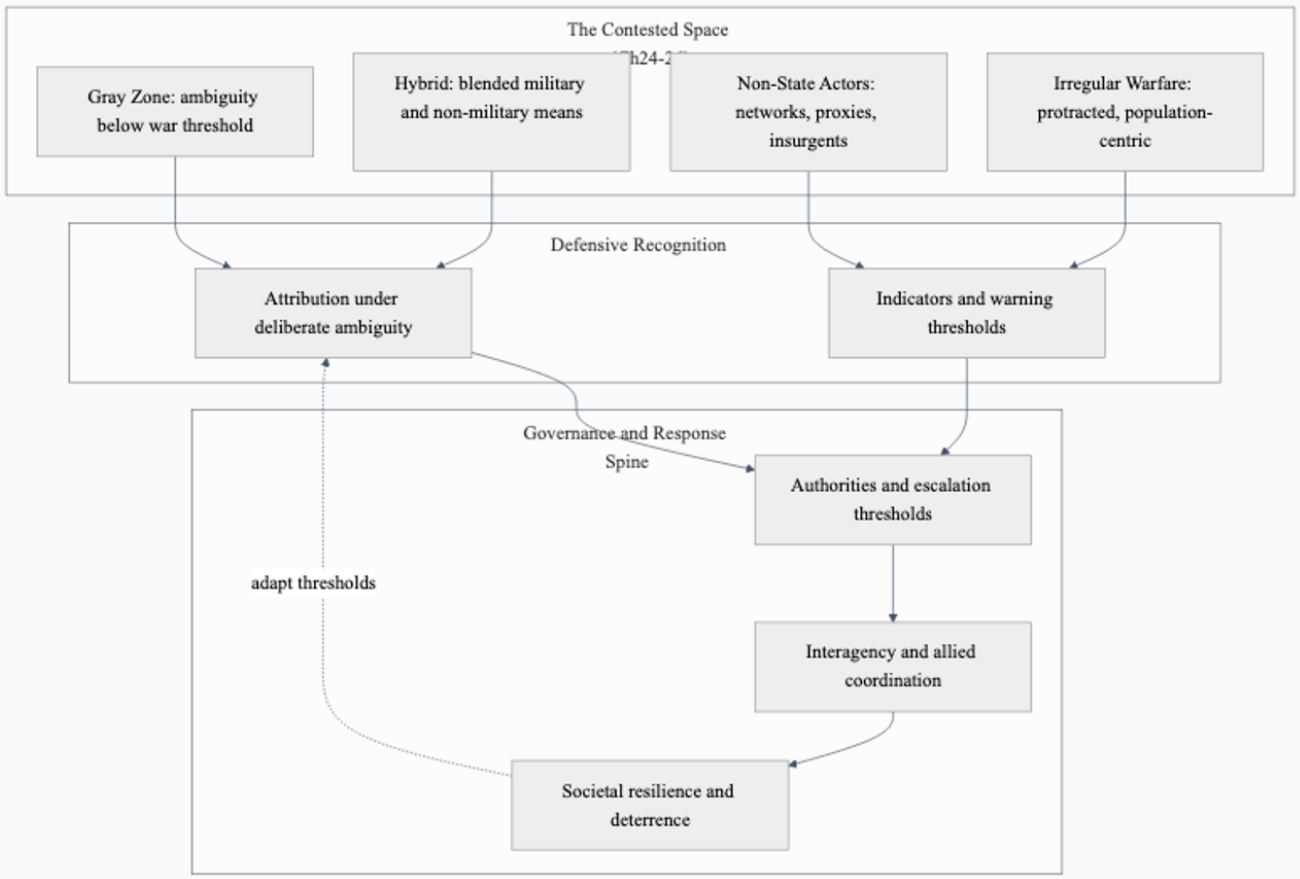


Figure 75: This part traces how the contested space below the threshold of war is recognized, attributed, and met through a defensive governance spine that ties authorities, coordination, and societal resilience back into sharper detection. The captioned view belongs to the gray zone hybrid warfare and non state actors section and should be read as a map of The Contested Space (Ch24-26), Gray Zone: ambiguity below war threshold, Hybrid: blended military and non-military means, and Non-State Actors: networks, proxies, insurgents, not as a capability score or live-task instruction.

36 Gray Zone Warfare

36.0.1 Gray Zone Warfare figures and course links: visual evidence, source flow, and navigation

The module uses Figure 76 and Figure 74 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 35, Section 37.
This module teaches the **Counterintelligence and Source-Integrity Defense** lane through a bounded, source-backed coursebook chapter. [239, 2026]; [247, 2026].

36.1 Counterintelligence and Source-Integrity Defense frame for Gray Zone Warfare: source context, topic focus, and reader task

Evidence anchor. Section 36; [239, 2026].

36.1.1 Gray Zone Warfare orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 36; [239, 2026].

36.1.2 Gray Zone Warfare conceptual primer: source context, core model, and reader task

This chapter teaches counterintelligence as source-integrity defense: the class studies how institutions protect evidence, people, access, and judgment from deception and compromise. The chapter uses **Dissemination-and-Marking Control Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**.
The central distinction is to separate defensive awareness from surveillance, handling, or operational security playbooks. Core topics include **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds; Chinese Gray Zone: Hybrid-threat indicator review using sample scenarios and policy thresholds**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [239, 2026]; [247, 2026].
Learners move from vocabulary and the **Dissemination-and-Marking Control Lens** distinction through topic lessons on **Hybrid-threat indicator review using sample scenarios and policy thresholds** with evidence and misconception checks, then assemble a **dissemination map with audience, caveat, marking, records, and feedback fields** with safety and rights gates.

36.1.3 Gray Zone Warfare learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 36; [239, 2026].

- Connect **Hybrid-threat indicator review using sample scenarios and policy thresholds and Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds** to **Counterintelligence and Source-Integrity Defense** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **dissemination map with audience, caveat, marking, records, and feedback fields** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate defensive awareness from surveillance, handling, or operational security playbooks; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as source compromise, deception acceptance, identity overconfidence, insider blind spots, and collapsing CI concerns into undifferentiated IT-security triage, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: CI content supports defensive awareness, source protection, and analytic integrity; it does not provide surveillance or handling playbooks.

36.1.4 Gray Zone Warfare core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 36; [239, 2026].

Term	Working definition
Source integrity	confidence that evidence has not been distorted, laundered, or compromised
Compromise signal	a clue that access, identity, or source reliability needs review
Corroboration	independent support that reduces single-source vulnerability
Insider risk	risk created by trusted access combined with motive, pressure, or control failure
Protected disclosure	a safe channel for reporting concerns without exposing sensitive details
Hybrid-threat indicator review using sample…	Key terms: Hybrid, threat, indicator.
Gray Zone Tactics: Hybrid-threat indicator…	Key terms: Gray, Zone, Tactics.

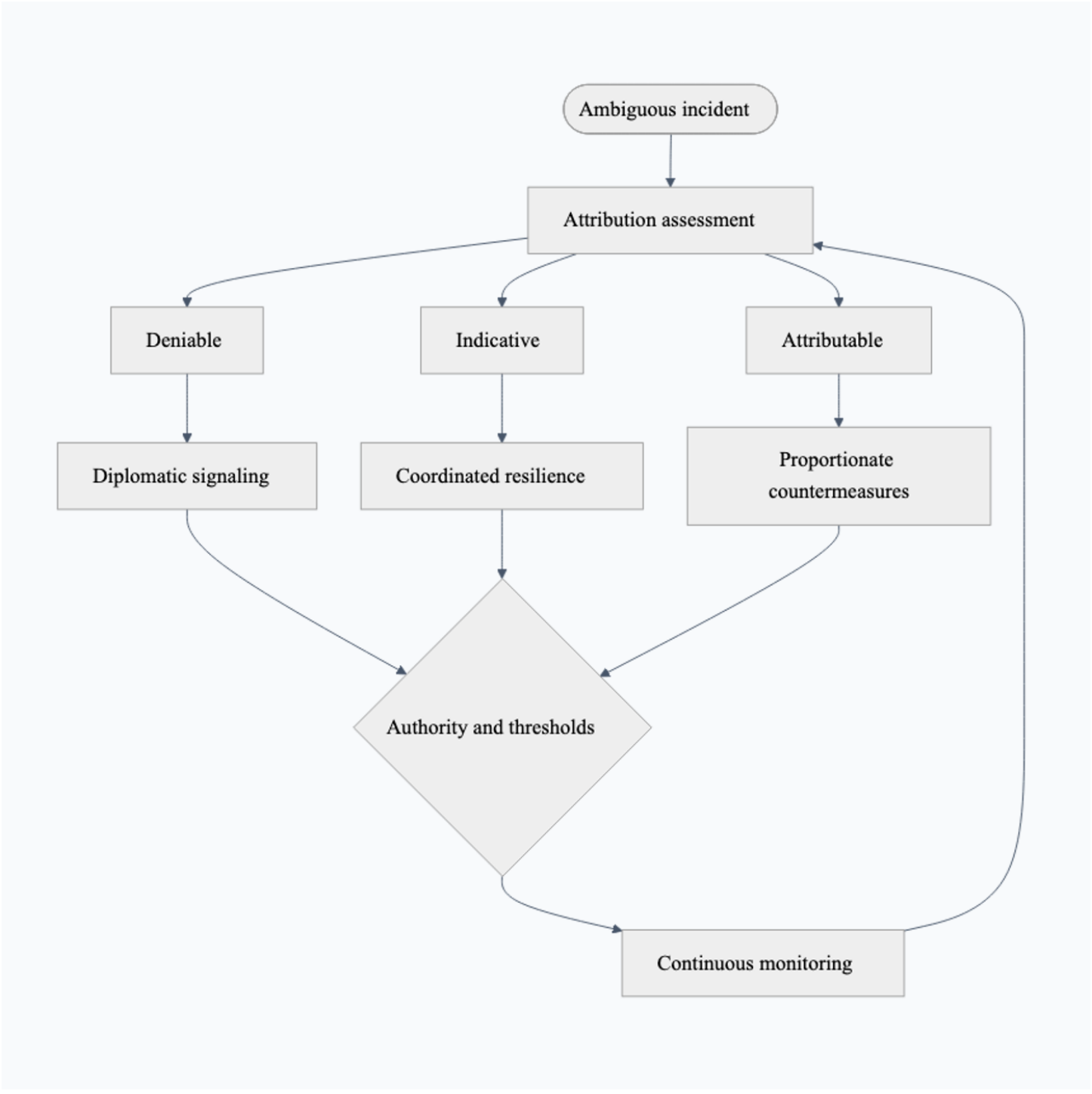


Figure 76: How ambiguous gray-zone activity is mapped onto rising attribution-confidence and response thresholds so that defensive options stay proportionate and governed. The captioned view belongs to the gray zone hybrid warfare and non state actors / gray zone warfare section and should be read as a map of Ambiguous incident, Attribution assessment, Deniable, and Indicative, not as a capability score or live-task instruction.

36.2 Dissemination-and-Marking Control Lens path for Gray Zone Warfare: lesson cluster, safe artifact, and review

Evidence anchor. Section 36; [239, 2026].

36.2.1 Gray Zone Warfare practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 36; [239, 2026].

36.2.2 Gray Zone Warfare topic lessons: source-backed concepts and transfer tasks

This module builds counterintelligence as source-integrity defense: the class studies how institutions protect evidence, people, access, and judgment from deception and compromise. The sequence opens with **Hybrid-threat indicator review using sample scenarios and policy thresholds**, **Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**, **Chinese Gray Zone: Hybrid-threat indicator review using sample scenarios and policy thresholds** and applies the **Dissemination-and-Marking Control Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 74; module overview Section 36; curriculum atlas Section 2.

Triangulation anchors. In module 24's topic-lessons section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

36.2.2.1 Lesson 1: Hybrid-threat indicator review using sample scenarios and policy thresholds

Concept. Hybrid-threat indicator review using sample scenarios and policy thresholds identifies hybrid indicators—proxy activity, ambiguous attribution, sub-threshold pressure—without prescribing response actions.

Why it matters. Hybrid-threat indicator review matters in the **Counterintelligence and Source-Integrity Defense** lane because deception-aware source review and defensive escalation evidence must stay separate from judgment; source compromise is a common failure.

Source support. Hybrid-threat indicator review using sample scenarios and policy thresholds rests on [109, 2026] and [110, 2026]. The lead source's own note reads: This is a peer-reviewed article in Connections: The Quarterly Journal (Vol. Use them for pinning down the scope of **Hybrid-threat indicator review using sample scenarios and policy thresholds**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. Read **Hybrid-threat indicator review** against the works cited for this row. [109, 2026] This is a peer-reviewed article in Connections: The Quarterly Journal (Vol. 21, No. 2, Spring 2022) by Peter Dobias and Kyle Christensen examining military competition below the threshold of armed conflict. It analyzes how Russia, China, and Iran operate in the space between peace and war, describing Russia's emphasis on information measures, China's maritime and force approaches, and Iran's anti-access and proxy strategies. [110, 2026] An article by Dr. Robert S. Burrell on the Irregular Warfare Initiative arguing that U.S. military doctrine inadequately addresses gray zone and hybrid warfare. It proposes a two-dimensional framework spanning peace-to-war and direct-to-indirect means, yielding four approaches: traditional warfare, deterrence, irregular warfare, and competition. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Hybrid-threat indicator review**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this deception-aware source review and defensive escalation topic. The artifact must name the indicator descriptor, the bounded claim about **Hybrid-threat indicator review using sample**, the attribution caveat, the threshold uncertainty, the non-attribution boundary, and the reviewer who approves the policy read. Shape **Hybrid-threat indicator review** work as an **ambiguous-threshold indicator matrix** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Hybrid-threat indicator review**: that activity falling below an obvious threshold is therefore ungoverned, rather than still bound by escalation limits and accountable review.

Transfer task. Transfer **Hybrid-threat indicator review** from this module to a second motif by preserving deception-aware source review and defensive escalation, replacing action with audit, and naming the blocked use.

36.2.2.2 Lesson 2: Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds

Concept. Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds identifies hybrid indicators—proxy activity, ambiguous attribution, sub-threshold pressure—without prescribing response actions.

Why it matters. Analysts use **Gray Zone Tactics** to separate defensive awareness from surveillance, handling, or operational security playbooks. A defensible treatment names the judgment it enables for deception-aware source review and defensive escalation review, the proof limit that source compromise would otherwise hide, and the reviewer accountable for challenge.

Source support. Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds rests on [111, 2026]. The most specific cited work observes: The piece is framed around adapting intelligence practice to contemporary competition short of war. Use it for pinning down the scope of **Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. Ground **Gray Zone Tactics** in the evidence the row cites. [111, 2026] An article in the U.S. Army's Military Intelligence Professional Bulletin on countering gray zone threats. It discusses how adversaries operate below the threshold of open conflict using hybrid activities across tactical, operational, and strategic levels, and considers how military intelligence can identify and attribute actors who attempt to remain anonymous. The piece is framed around adapting intelligence practice to contemporary competition short of war. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Gray Zone Tactics**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this deception-aware source review and defensive escalation topic. The artifact must name the indicator descriptor, the bounded claim about **Gray Zone Tactics**, the attribution caveat, the threshold uncertainty, the non-attribution boundary, and the reviewer who approves the policy read. Shape **Gray Zone Tactics** work as an **ambiguous-threshold indicator matrix** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Gray Zone Tactics**: that activity falling below an obvious threshold is therefore ungoverned, rather than still bound by escalation limits and accountable review.

Transfer task. Reuse the **Gray Zone Tactics** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

36.2.2.3 Lesson 3: Chinese Gray Zone: Hybrid-threat indicator review using sample scenarios and policy thresholds

Concept. Chinese Gray Zone: Hybrid-threat indicator review using sample scenarios and policy thresholds identifies hybrid indicators—proxy activity, ambiguous attribution, sub-threshold pressure—without prescribing response actions.

Why it matters. Analysts use **Chinese Gray Zone** to separate defensive awareness from surveillance, handling, or operational security playbooks. A defensible treatment names the judgment it enables for deception-aware source review and defensive escalation review, the proof limit that source compromise would otherwise hide, and the reviewer accountable for challenge.

Source support. Chinese Gray Zone: Hybrid-threat indicator review using sample scenarios and policy thresholds rests on [308, 2026] and [311, 2026]. The closest source to this row notes: An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. Use them for pinning down the scope of **Chinese Gray Zone: Hybrid-threat indicator review using sample scenarios and policy thresholds**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. Ground **Chinese Gray Zone** in the evidence the row cites. [308, 2026] An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure. [311, 2026] An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Chinese Gray Zone**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this deception-aware source review and defensive escalation topic. The artifact must name the indicator descriptor, the bounded claim about **Chinese Gray Zone**, the attribution caveat, the threshold uncertainty, the non-attribution boundary, and the reviewer who approves the policy read. Shape **Chinese Gray Zone** work as an **ambiguous-threshold indicator matrix** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Chinese Gray Zone**: that activity falling below an obvious threshold is therefore ungoverned, rather than still bound by escalation limits and accountable review.

Transfer task. Reuse the **Chinese Gray Zone** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

36.2.2.4 Lesson 4: Russian Hybrid Warfare: Hybrid-threat indicator review using sample scenarios and policy thresholds

Concept. Russian Hybrid Warfare: Hybrid-threat indicator review using sample scenarios and policy thresholds identifies hybrid indicators—proxy activity, ambiguous attribution, sub-threshold pressure—without prescribing response actions.

Why it matters. Without explicit treatment of **Russian Hybrid Warfare**, source compromise undermines deception-aware source review and defensive escalation review; the lesson builds the habit to separate defensive awareness from surveillance, handling, or operational security playbooks.

Source support. Russian Hybrid Warfare: Hybrid-threat indicator review using sample scenarios and policy thresholds rests on [111, 2026]. Its anchor reference records: The piece is framed around adapting intelligence practice to contemporary competition short of war. Use it for the working definition that **Russian Hybrid Warfare: Hybrid-threat indicator review using sample scenarios and policy thresholds** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. Ground **Russian Hybrid Warfare** in the evidence the row cites. [111, 2026] An article in the U.S. Army's Military Intelligence Professional Bulletin on countering gray zone threats. It discusses how adversaries operate below the threshold of open conflict using hybrid activities across tactical, operational, and strategic levels, and considers how military intelligence can identify and attribute actors who attempt to remain anonymous. The piece is framed around adapting intelligence practice to contemporary competition short of war. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Russian Hybrid Warfare**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this deception-aware source review and defensive escalation topic. The artifact must name the indicator descriptor, the bounded claim about **Russian Hybrid Warfare**, the attribution caveat, the threshold uncertainty, the non-attribution boundary, and the reviewer who approves the policy read. Shape **Russian Hybrid Warfare** work as an **ambiguous-threshold indicator matrix** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Russian Hybrid Warfare**: that activity falling below an obvious threshold is therefore ungoverned, rather than still bound by escalation limits and accountable review.

Transfer task. Transfer **Russian Hybrid Warfare** from this module to a second motif by preserving deception-aware source review and defensive escalation, replacing action with audit, and naming the blocked use.

36.2.2.5 Lesson 5: Anonymous: Hybrid-threat indicator review using sample scenarios and policy thresholds

Concept. Anonymous: Hybrid-threat indicator review using sample scenarios and policy thresholds identifies hybrid indicators—proxy activity, ambiguous attribution, sub-threshold pressure—without prescribing response actions.

Why it matters. Anonymous: Hybrid-threat indicator review using sample scenarios and policy thresholds connects classroom vocabulary to Counterintelligence and Source-Integrity Defense practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Anonymous: Hybrid-threat indicator review using sample scenarios and policy thresholds rests on [111, 2026]. The lead source's own note reads: Army's Military Intelligence Professional Bulletin on countering gray zone threats. Use it for the working definition that **Anonymous: Hybrid-threat indicator review using sample scenarios and policy thresholds** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. For **Anonymous: Hybrid-threat indicator review using sample scenarios and policy thresholds**, reason from the sources cited in this row. [111, 2026] An article in the U.S. Army's Military Intelligence Professional Bulletin on countering gray zone threats. It discusses how adversaries operate below the threshold of open conflict using hybrid activities across tactical, operational, and strategic levels, and considers how military intelligence can identify and attribute actors who attempt to remain anonymous. The piece is framed around adapting intelligence practice to contemporary competition short of war. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Anonymous**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this deception-aware source review and defensive escalation topic. The artifact must name the indicator descriptor, the bounded claim about **Anonymous**, the attribution caveat, the threshold uncertainty, the non-attribution boundary, and the reviewer who approves the policy read. Shape **Anonymous: Hybrid-threat indicator review using sample scenarios and policy thresholds** work as an **ambiguous-threshold indicator matrix** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Anonymous: Hybrid-threat indicator review using sample scenarios and policy thresholds**: that activity falling below an obvious threshold is therefore ungoverned, rather than still bound by escalation limits and accountable review.

Transfer task. Reuse the **Anonymous: Hybrid-threat indicator review using sample scenarios and policy thresholds** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

36.2.2.6 Lesson 6: Full Spectrum Conflict Design: Hybrid-threat indicator review using sample scenarios and policy thresholds

Concept. Full Spectrum Conflict Design: Hybrid-threat indicator review using sample scenarios and policy thresholds identifies ambiguous-threshold activity through indicators, attribution caution, and policy review—not through prescribed response actions.

Why it matters. Analysts use **Full Spectrum Conflict Design** to separate defensive awareness from surveillance, handling, or operational security playbooks. A defensible treatment names the judgment it enables for deception-aware source review and defensive escalation review, the proof limit that source compromise would otherwise hide, and the reviewer accountable for challenge.

Source support. Full Spectrum Conflict Design: Hybrid-threat indicator review using sample scenarios and policy thresholds rests on [110, 2026]. The most specific cited work observes: Burrell on the Irregular Warfare Initiative arguing that U.S. Use it for fixing what **Full Spectrum Conflict Design: Hybrid-threat indicator review using sample scenarios and policy thresholds** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. Read **Full Spectrum Conflict Design** against the works cited for this row. [110, 2026] An article by Dr. Robert S. Burrell on the Irregular Warfare Initiative arguing that U.S. military doctrine inadequately addresses gray zone and hybrid warfare. It proposes a two-dimensional framework spanning peace-to-war and direct-to-indirect means, yielding four approaches: traditional warfare, deterrence, irregular warfare, and competition. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Full Spectrum Conflict Design**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this deception-aware source review and defensive escalation topic. The artifact must name the indicator descriptor, the bounded claim about **Full Spectrum Conflict Design**, the attribution caveat, the threshold uncertainty, the non-attribution boundary, and the reviewer who approves the policy read. Shape **Full Spectrum Conflict Design** work as an **ambiguous-threshold indicator matrix** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Full Spectrum Conflict Design**: that activity falling below an obvious threshold is therefore ungoverned, rather than still bound by escalation limits and accountable review.

Transfer task. Transfer **Full Spectrum Conflict Design** from this module to a second motif by preserving deception-aware source review and defensive escalation, replacing action with audit, and naming the blocked use.

36.2.3 Gray Zone Warfare worked safe example: synthetic inputs, evidence, and review

Worked example: a sample research lab reviews a synthetic source-quality anomaly after a disputed report. [239, 2026]; [247, 2026].

Triangulation anchors. In module 24's worked-example section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **hybrid-threat governance**. Learners use a **ambiguous-threshold indicator matrix** and keep this boundary visible: No live targeting, covert action, retaliation planning, or attribution certainty beyond evidence.

Frame. The classroom question centers on **Hybrid-threat indicator review using sample scenarios and policy thresholds**. Excluded actions stay explicit, and the **Dissemination-and-Marking Control Lens** planning question is: Which audience, release authority, marking vocabulary, records duty, and feedback loop governs this intelligence artifact?

Inputs. For the **Hybrid-threat indicator review using sample scenarios and policy thresholds** scenario, use toy access logs, public policy excerpts, synthetic source notes, and a reviewer escalation path. The Dissemination-and-Marking Control Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Hybrid-threat indicator review using sample scenarios and policy thresholds**, students separate identity from access, list anomaly hypotheses, seek corroboration, and route sensitive concerns to review. Pause whenever an inference about Hybrid-threat indicator review using sample scenarios and policy thresholds appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Hybrid-threat indicator review using sample scenarios and policy thresholds** classroom scenario; unit artifact = ambiguous-threshold indicator matrix; evidence = allowed inputs; method = deception-aware source review and defensive escalation; output = a source-integrity memo with competing explanations, confidence, protected-disclosure note, and next-review owner; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Hybrid-threat indicator review using sample scenarios and policy thresholds** as "Dissemination-and-Marking Control Lens confirms it" is not enough. The revision ties the claim to deception-aware source review and defensive escalation, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Hybrid-threat indicator review using sample scenarios and policy thresholds** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

36.2.4 Gray Zone Warfare practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Dissemination-and-Marking Control Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**.

Triangulation anchors. In module 24's practice-sequence section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Hybrid-threat indicator review using sample scenarios and policy thresholds, Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds, Chinese Gray Zone: Hybrid-threat indicator review using sample scenarios and policy thresholds; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Counterintelligence and Source-Integrity Defense** lane.
2. Frame	Answer the lens question: Which audience, release authority, marking vocabulary, records duty, and feedback loop governs this intelligence artifact?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.

Move	Learner action	Output	Check
3. Evidence	Fill the artifact fields for Hybrid-threat indicator review using sample scenarios and policy thresholds: dissemination map with audience, caveat, marking, records, and feedback fields.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the ambiguous-threshold indicator matrix fields for Hybrid-threat indicator review using sample scenarios and policy thresholds.	Unit profile note.	Evidence artifacts include threshold indicator, attribution caveat.
4. Challenge	Test the misconception that activity falling below an obvious threshold is therefore ungoverned, rather than still bound by escalation limits and accountable review.	Failure-mode note.	The artifact applies the key distinction: separate defensive awareness from surveillance, handling, or operational security playbooks.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

36.2.4.1 Gray Zone Warfare instructor notes: source reasoning, review points, and studio focus Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**. [239, 2026]; [247, 2026].

36.2.4.2 Gray Zone Warfare extension exercise: peer validation and refresh trigger review **Evidence anchor.** Section 36; [239, 2026]. Have learners swap artifacts and apply the **Dissemination-and-Marking Control Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**.

36.2.5 Gray Zone Warfare knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 36; [239, 2026].

1. Explain how **Hybrid-threat indicator review using sample scenarios and policy thresholds** is defined here; name the source descriptor that supports the definition.
2. Contrast **Hybrid-threat indicator review using sample scenarios and policy thresholds** with **Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds** using the **Dissemination-and-Marking Control Lens** artifact fields.
3. Identify one failure mode from the **Counterintelligence and Source-Integrity Defense** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which explanation preserves uncertainty without ignoring a possible compromise signal?
5. Correct this misconception: that activity falling below an obvious threshold is therefore ungoverned, rather than still bound by escalation limits and accountable review.

36.2.5.1 Gray Zone Warfare answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Hybrid-threat indicator review using sample scenarios and policy thresholds** without source evidence, uncertainty, or a safe transfer task.

36.3 Gray Zone Warfare assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 36; [239, 2026].

36.3.1 Gray Zone Warfare evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 36; [239, 2026].

36.3.2 Gray Zone Warfare transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 36; [239, 2026].

36.3.2.1 Gray Zone Warfare lineage and source tradition: profile, concepts, and first anchors This sits in the **Counterintelligence and Source-Integrity Defense** lineage: defending institutions, sources, and judgments against deception, insider risk, foreign-intelligence targeting, and source contamination. [239, 2026]; [247, 2026].

36.3.2.2 Gray Zone Warfare working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 36; [239, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**, with provenance and reviewability throughout.

36.3.2.3 Gray Zone Warfare knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [239, 2026]; [247, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

36.3.2.4 Gray Zone Warfare transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 36; [239, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**.
- **Evidence contract:** keep the **Counterintelligence and Source-Integrity Defense** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

36.3.2.5 Gray Zone Warfare profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 36; [239, 2026].

The matched profile emphasizes defending institutions, sources, and judgments against deception, insider risk, foreign-intelligence targeting, and source contamination. The method stack is threat awareness, source-descriptor audit, corroboration, anomaly review, red-team challenge, and protected disclosure paths; the local topic cluster is **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**.

36.3.3 Gray Zone Warfare evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 36; [239, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Counterintelligence and Source-Integrity Defense** profile tells reviewers what evidence is strong enough for the module artifact built around **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**.

36.3.3.1 Gray Zone Warfare guide source spine: inherited keys and local citation roles Primary guide citations: [239, 2026]; [247, 2026]; [249, 2026]; [275, 2026]; [276, 2026]; [283, 2026]; [286, 2026]; [293, 2026]; [295, 2026]; [109, 2026]; [110, 2026]; [111, 2026]; [308, 2026]; [311, 2026].

36.3.3.2 Gray Zone Warfare verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [239, 2026]; [247, 2026].

Tier	What counts	How it is used
Source guide	[239, 2026]; [247, 2026]; [249, 2026]; [275, 2026]; [276, 2026]; [283, 2026]; [286, 2026]; [293, 2026]; [295, 2026]; [109, 2026]; [110, 2026]; [111, 2026]; [308, 2026]; [311, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 24's source-canon section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds** and [239, 2026]; [247, 2026], but only directly verified source URLs are encoded as citations.

36.3.3.3 Gray Zone Warfare intelligence practice lens: evidence artifact and safety check Practice lens: **Dissemination-and-Marking Control Lens** for **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**. [239, 2026]; [247, 2026].

Planning question: Which audience, release authority, marking vocabulary, records duty, and feedback loop governs this intelligence artifact?

Evidence artifact: dissemination map with audience, caveat, marking, records, and feedback fields.

Validation rule: verify source authority, public/classification status, CAPCO-safe vocabulary, audience need, and records disposition before reuse. Applied to **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**.

Handoff contract: deliver release-neutral summaries, source metadata, marking rationale, and review ownership as separate fields.

Safety check: exclude classified content, live release decisions, source-method exposure, and improvised control markings.

36.3.3.4 Gray Zone Warfare runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 36; [239, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	24.99	24.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Gray Zone Warfare to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Bounded autonomy, procurement, incident-response, and assurance studio	24.101	24.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Gray Zone Warfare	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Model-card, recoverability, retention, and learner-support evidence package	24.102	24.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Gray Zone Warfare	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Hybrid-threat indicator review using sample scenarios and policy thresholds	24.1	24.1 source title transformed into safe curriculum treatment; original: Defining the Gray Zone: Between Peace and War	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Hybrid-threat indicator review using sample scenarios and policy thresholds	24.2	24.2 source title transformed into safe curriculum treatment; original: Gray Zone Tactics: Competition, Crisis, and Conflict	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Hybrid-threat indicator review using sample scenarios and policy thresholds	24.3	24.3 source title transformed into safe curriculum treatment; original: Chinese Gray Zone: South China Sea and Taiwan Straits	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Hybrid-threat indicator review using sample scenarios and policy thresholds	24.4	24.4 source title transformed into safe curriculum treatment; original: Russian Hybrid Warfare: Ukraine, Baltic States, Information Domain	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Hybrid-threat indicator review using sample scenarios and policy thresholds	24.5	24.5 source title transformed into safe curriculum treatment; original: Anonymous No More: Countering Gray Zone Threats (MIPB 2025)	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Hybrid-threat indicator review using sample scenarios and policy thresholds	24.6	24.6 source title transformed into safe curriculum treatment; original: Full Spectrum Conflict Design (IWI 2025)	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings

36.3.3.5 Gray Zone Warfare reusable subsection contract: topic rows, artifacts, and safety duties **Evidence anchor.** Section 36; [239, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Hybrid-threat indicator review using sample scenarios and policy thresholds	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Chinese Gray Zone: Hybrid-threat indicator review using sample scenarios and policy thresholds	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Russian Hybrid Warfare: Hybrid-threat indicator review using sample scenarios and policy thresholds	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Anonymous: Hybrid-threat indicator review using sample scenarios and policy thresholds	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Full Spectrum Conflict Design: Hybrid-threat indicator review using sample scenarios and policy thresholds	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings

36.3.3.6 Gray Zone Warfare annotated source ledger: real titles and local contribution Each source cited by this **Counterintelligence and Source-Integrity Defense** module is paired below with its real title and a one-line note on what it contributes to **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**.

Source	Cited work	What it contributes	Status
[239, 2026]	Digital Space and Human Rights	Official OHCHR digital rights portal.	original source-guide
[247, 2026]	AI in the Public Sector	Official OECD.AI public-sector AI theme page.	original source-guide

Source	Cited work	What it contributes	Status
[249, 2026]	GovTech: Putting People First	The official page for the World Bank's Global Program on GovTech and Public Sector Innovation, which helps governments use technology and data to improve public services and governance. It describes support for digital transformation in public administration across areas such as tax administration, public financial management, human resource systems, and citizen engagement, with cross-cutting themes including responsible AI and green digital transformation.	verified source-guide
[275, 2026]	Fact Sheet: New Rule on the Accessibility of Web Content and Mobile Apps Provided by State and Local Governments	A US Department of Justice fact sheet explaining the 2024 ADA Title II rule requiring state and local governments to make their web content and mobile apps accessible. It establishes WCAG 2.1 Level AA as the technical standard, applies to entities such as schools, courts, libraries, and transit agencies, and sets compliance deadlines of April 2027 for larger jurisdictions and April 2028 for smaller ones.	verified source-guide
[276, 2026]	What is a Data Protection Impact Assessment and When Is This Mandatory?	A European Data Protection Board FAQ page, part of its data protection guide for small businesses, explaining Data Protection Impact Assessments (DPIAs) and when they are mandatory. It describes a DPIA as a written assessment of the impact of a planned processing operation, required when processing poses high risks to individuals' rights.	verified source-guide
[283, 2026]	Recommendation of the Council on Open Government	An OECD legal instrument document reproducing the Recommendation of the Council on Open Government (OECD/LEGAL/0438), adopted on 14 December 2017. It defines open government as a culture of governance promoting transparency, integrity, accountability, and stakeholder participation in support of democracy and inclusive growth.	verified source-guide
[286, 2026]	Model Cards for Model Reporting	The arXiv abstract for "Model Cards for Model Reporting" (2018) by Mitchell, Wu, Zaldivar, and colleagues, which introduces a framework for transparent documentation of machine learning models. Model cards are short accompanying documents that report a model's benchmarked performance across varied conditions, including different cultural, demographic, and phenotypic groups, along with intended use, evaluation methodology, and deployment considerations.	verified source-guide

Source	Cited work	What it contributes	Status
[293, 2026]	Inventory of NARA Artificial Intelligence (AI) Use Cases	The National Archives and Records Administration (NARA) official inventory of its artificial intelligence use cases, documenting 14 projects across deployed, pilot, and planned stages. Deployed efforts include workplace productivity tools, automated tagging for museum experiences, and historical record retrieval, while pilots cover PII detection and redaction, semantic search, and metadata generation, and planned work targets FOIA processing and public search.	verified source-guide
[295, 2026]	M-25-22: Driving Efficient Acquisition of Artificial Intelligence in Government	OMB Memorandum M-25-22 (April 3, 2025), Driving Efficient Acquisition of Artificial Intelligence in Government, issued under Executive Order 13960 and related directives. It provides guidance to federal agencies for acquiring effective and trustworthy AI in a timely, cost-effective manner, and rescinds and replaces earlier memorandum M-24-18.	verified source-guide
[109, 2026]	The 'Grey Zone' and Hybrid Activities	This is a peer-reviewed article in Connections: The Quarterly Journal (Vol. 21, No. 2, Spring 2022) by Peter Dobias and Kyle Christensen examining military competition below the threshold of armed conflict. It analyzes how Russia, China, and Iran operate in the space between peace and war, describing Russia's emphasis on information measures, China's maritime and force approaches, and Iran's anti-access and proxy strategies.	verified source-guide
[110, 2026]	A Full Spectrum of Conflict Design: How Doctrine Should Embrace	An article by Dr. Robert S. Burrell on the Irregular Warfare Initiative arguing that U.S. military doctrine inadequately addresses gray zone and hybrid warfare. It proposes a two-dimensional framework spanning peace-to-war and direct-to-indirect means, yielding four approaches: traditional warfare, deterrence, irregular warfare, and competition.	verified source-guide
[111, 2026]	Anonymous No More: Countering the Gray Zone Threat - from MIPB	An article in the U.S. Army's Military Intelligence Professional Bulletin on countering gray zone threats. It discusses how adversaries operate below the threshold of open conflict using hybrid activities across tactical, operational, and strategic levels, and considers how military intelligence can identify and attribute actors who attempt to remain anonymous. The piece is framed around adapting intelligence practice to contemporary competition short of war.	verified source-guide
[308, 2026]	Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure	An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure.	verified source-guide

Source	Cited work	What it contributes	Status
[311, 2026]	Countering Information Threats	An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering.	verified source-guide

Where this sits. This module's overview is Section 36; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

36.3.4 Gray Zone Warfare governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 36; [239, 2026].

36.3.5 Gray Zone Warfare analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 24's governance-boundary section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **Counterintelligence and Source-Integrity Defense** for **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**. [239, 2026]; [247, 2026].

Curriculum topic spine: Hybrid-threat indicator review using sample scenarios and policy thresholds, **Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**, **Chinese Gray Zone: Hybrid-threat indicator review using sample scenarios and policy thresholds**. **Verified anchor cluster:** [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]; [Agency, 2009]; [Jr., 2007]; [Burkett, 2013].

Conceptual depth: defending institutions, sources, and judgments against deception, insider risk, foreign-intelligence targeting, and source contamination.

Method stack: threat awareness, source-descriptor audit, corroboration, anomaly review, red-team challenge, and protected disclosure paths.

Composability contract: identity, access, reporting, corroboration, caveats, and confidence are modeled independently so defensive review can happen without exposure.

Known failure modes: source compromise, deception acceptance, identity overconfidence, insider blind spots, and collapsing CI concerns into undifferentiated IT-security triage.

Defensive boundary: CI content supports defensive awareness, source protection, and analytic integrity; it does not provide surveillance or handling playbooks. Applied to **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**.

Anchor	Why it matters here
[Counterintelligence and Center, 2024]	Official strategy for defensive CI integration, foreign-intelligence threat awareness, strategic advantage protection, and future readiness. Checked as of 2026-05-21; role: curriculum_anchor.
[Archives and Administration, 1981]	Official legal anchor for intelligence authorities, rights-aware collection, analytic competition, oversight, and source-method protection. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026d]	Official sourcing directive for traceability, citations, source descriptors, and source summaries. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2015]	Official ODNI analytic tradecraft standards directive. Checked as of 2026-05-21; role: source_quality_anchor.
[Agency, 2009]	Official structured analytic techniques primer for bias checks, alternatives, and warning analysis. Checked as of 2026-05-21; role: curriculum_anchor.
[Jr., 2007]	Foundational analytic cognition source for bias, mental models, and structured reasoning. Checked as of 2026-06-06; role: curriculum_anchor.
[Burkett, 2013]	A CIA Studies in Intelligence analyst essay arguing that the traditional MICE recruitment-motivation model (Money, Ideology, Compromise, Ego) is better understood through Cialdini's influence principles reframed as RASCLS (Reciprocation, Authority, Scarcity, Commitment/Consistency, Liking, Social Proof), grounding the historical and conceptual lineage of HUMINT recruitment frameworks. Checked as of 2026-06-08; role: curriculum_anchor.

36.3.5.1 Gray Zone Warfare evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **Counterintelligence and Source-Integrity Defense** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [239, 2026]; [247, 2026].

36.3.6 Gray Zone Warfare agentic boundary: assist, approve, block, and record

Evidence anchor. Section 36; [239, 2026].

AGEINT translation is bounded by the **Counterintelligence and Source-Integrity Defense** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**.

36.3.6.1 Gray Zone Warfare permitted defensive utility: curriculum uses and safe outputs

Evidence anchor. Section 36; [239, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**.

36.3.6.2 Gray Zone Warfare excluded operational boundary: blocked actions and stop rules

Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [239, 2026]; [247, 2026] and **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

36.3.7 Gray Zone Warfare governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 36; [239, 2026].
Governance is practiced as a gate on the **Counterintelligence and Source-Integrity Defense** lane. Learners use the **Dissemination-and-Marking Control Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**.

36.3.7.1 Gray Zone Warfare governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [239, 2026]; [247, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Counterintelligence and Source-Integrity Defense** failure modes and the **Dissemination-and-Marking Control Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

36.3.7.2 Gray Zone Warfare evidence package handoff: appendices, records, and reuse

Evidence anchor. Section 36; [239, 2026].
Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Dissemination-and-Marking Control Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**.

36.3.7.3 Gray Zone Warfare current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**. [239, 2026]; [247, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_ncsc_counterintelligence_strategy` for **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**?	The National Counterintelligence Strategy; lane `counterintelligence_source_integrity`; checked 2026-05-21.	dissemination map with audience, caveat, marking, records, and feedback fields; Official strategy for defensive CI integration, foreign-intelligence threat awareness, strategic advantage protection, and future readiness.
What does the module inherit from `official_odni_eo_12333` for **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**?	Executive Order 12333: United States Intelligence Activities; lane `legal_oversight`; checked 2026-05-21.	dissemination map with audience, caveat, marking, records, and feedback fields; Official legal anchor for intelligence authorities, rights-aware collection, analytic competition, oversight, and source-method protection.
What does the module inherit from `official_odni_icd_206` for **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**?	Intelligence Community Directive 206: Sourcing Requirements for Disseminated Analytic Products; lane `analytic_tradecraft`; checked 2026-05-21.	dissemination map with audience, caveat, marking, records, and feedback fields; Official sourcing directive for traceability, citations, source descriptors, and source summaries.
What does the module inherit from `official_odni_icd_203` for **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**?	Intelligence Community Directive 203: Analytic Standards; lane `source_quality_spine`; checked 2026-05-21.	dissemination map with audience, caveat, marking, records, and feedback fields; Official ODNI analytic tradecraft standards directive.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 36; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

36.3.8 Gray Zone Warfare assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 36; [239, 2026].

36.3.9 Gray Zone Warfare assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 36; [239, 2026].

36.3.9.1 Gray Zone Warfare capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds** and [239, 2026]; [247, 2026].

36.3.9.2 Gray Zone Warfare instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds** and [239, 2026]; [247, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

36.3.9.3 Gray Zone Warfare assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Hybrid-threat indicator review using sample scenarios and policy thresholds	Completed **dissemination map with audience, caveat, marking, records, and feedback fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds	Completed **dissemination map with audience, caveat, marking, records, and feedback fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Chinese Gray Zone: Hybrid-threat indicator review using sample scenarios and policy thresholds	Completed **dissemination map with audience, caveat, marking, records, and feedback fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

36.3.10 Gray Zone Warfare refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [239, 2026]; [247, 2026] and **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**.

36.3.10.1 Gray Zone Warfare refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**. The local signals begin with [239, 2026]; [247, 2026].

36.3.10.2 Gray Zone Warfare claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**, and the source spine for these checks begins with [239, 2026]; [247, 2026].

36.3.11 Gray Zone Warfare reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [239, 2026]; [247, 2026].

Triangulation anchors. In module 24's review-checklist section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds**. [239, 2026]; [247, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.

- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

36.3.12 Gray Zone Warfare learning-path links: module map, overview, and curriculum atlas

These links keep **Hybrid-threat indicator review using sample scenarios and policy thresholds; Gray Zone Tactics: Hybrid-threat indicator review using sample scenarios and policy thresholds** paired with the orientation atlas, the parent unit, and the previous and next modules, so a reader can trace which claims and caveats are inherited rather than re-derived here. Anchored at [239, 2026]; [247, 2026].
Section 2, Section 35, Section 37

37 Non-State Actor Intelligence

37.0.1 Non-State Actor Intelligence figures and course links: visual evidence, source flow, and navigation

The module uses Figure 77 and Figure 74 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 35, Section 36, Section 38.
This module teaches the **Counterintelligence and Source-Integrity Defense** lane through a bounded, source-backed coursebook chapter. [238, 2026]; [247, 2026].

37.1 Counterintelligence and Source-Integrity Defense frame for Non-State Actor Intelligence: source context, topic focus, and reader task

Evidence anchor. Section 37; [238, 2026].

37.1.1 Non-State Actor Intelligence orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 37; [238, 2026].

37.1.2 Non-State Actor Intelligence conceptual primer: source context, core model, and reader task

This chapter teaches counterintelligence as source-integrity defense: the class studies how institutions protect evidence, people, access, and judgment from deception and compromise. The chapter uses **Dissemination-and-Marking Control Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**.
The central distinction is to separate defensive awareness from surveillance, handling, or operational security playbooks. Core topics include **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds; Private Military Corporations as Intelligence: Hybrid-threat indicator review using sample scenarios and policy thresholds**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [238, 2026]; [247, 2026].
Learners move from vocabulary and the **Dissemination-and-Marking Control Lens** distinction through topic lessons on **Financial due-diligence typology exercise using synthetic records and compliance boundaries** with evidence and misconception checks, then assemble a **dissemination map with audience, caveat, marking, records, and feedback fields** with safety and rights gates.

37.1.3 Non-State Actor Intelligence learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 37; [238, 2026].

- Connect **Financial due-diligence typology exercise using synthetic records and compliance boundaries and Hybrid-threat indicator review using sample scenarios and policy thresholds** to **Counterintelligence and Source-Integrity Defense** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **dissemination map with audience, caveat, marking, records, and feedback fields** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate defensive awareness from surveillance, handling, or operational security playbooks; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as source compromise, deception acceptance, identity overconfidence, insider blind spots, and collapsing CI concerns into undifferentiated IT-security triage, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: CI content supports defensive awareness, source protection, and analytic integrity; it does not provide surveillance or handling playbooks.

37.1.4 Non-State Actor Intelligence core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 37; [238, 2026].

Term	Working definition
Source integrity	confidence that evidence has not been distorted, laundered, or compromised
Compromise signal	a clue that access, identity, or source reliability needs review
Corroboration	independent support that reduces single-source vulnerability
Insider risk	risk created by trusted access combined with motive, pressure, or control failure
Protected disclosure	a safe channel for reporting concerns without exposing sensitive details
Financial due-diligence typology exercise using…	Key terms: Financial, due, diligence.
Hybrid-threat indicator review using sample…	Key terms: Hybrid, threat, indicator.

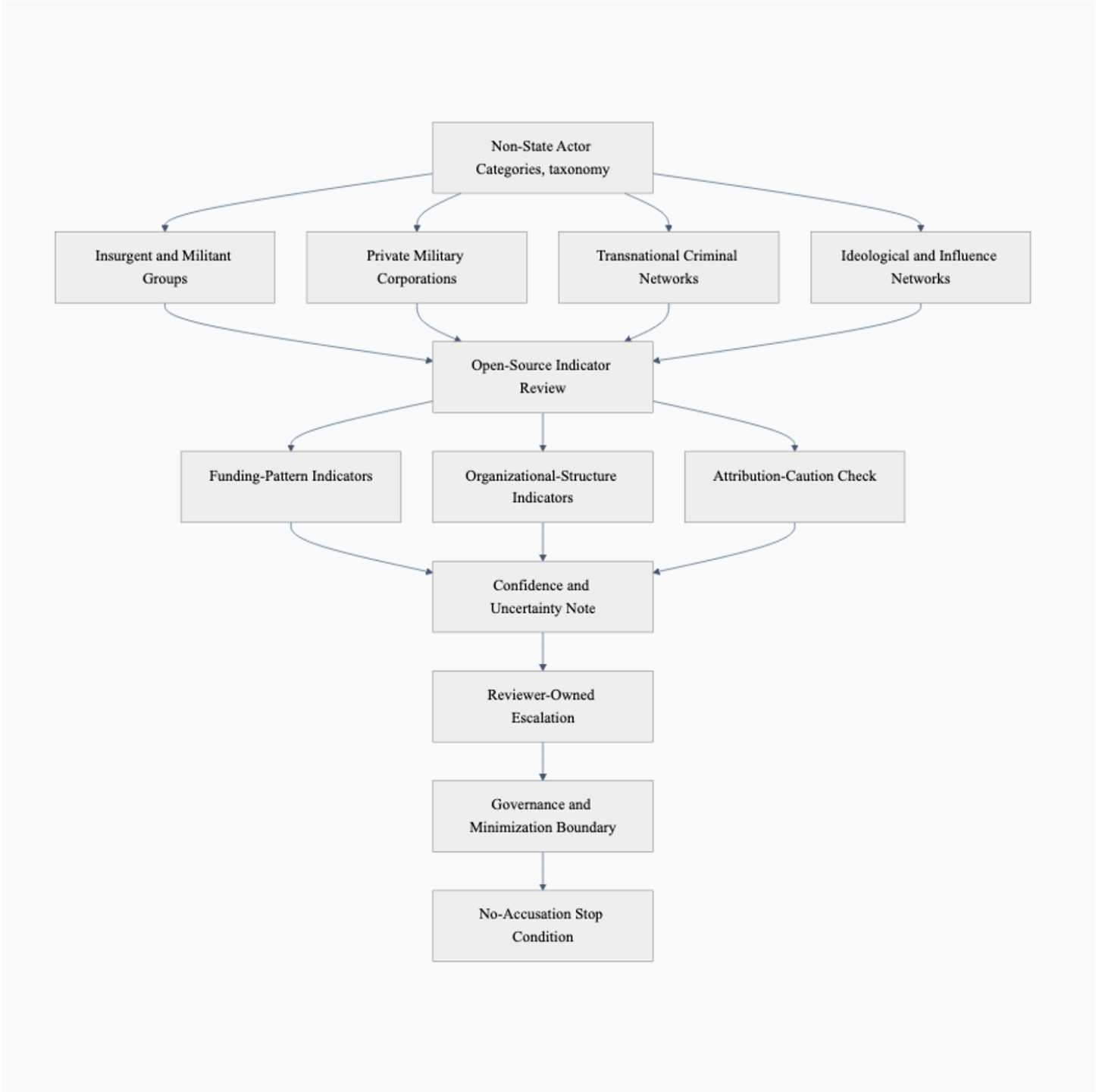


Figure 77: A defensive classification of non-state actor categories feeding an attribution-cautious indicator review with reviewer-owned escalation and governance boundaries. It is anchored to the gray zone hybrid warfare and non state actors / non state actor intelligence section; use it to inspect Non-State Actor Categories, taxonomy, Insurgent and Militant Groups, Private Military Corporations, and Transnational Criminal Networks while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

37.2 Dissemination-and-Marking Control Lens path for Non-State Actor Intelligence: lesson cluster, safe artifact, and review

Evidence anchor. Section 37; [238, 2026].

37.2.1 Non-State Actor Intelligence practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 37; [238, 2026].

37.2.2 Non-State Actor Intelligence topic lessons: source-backed concepts and transfer tasks

This module builds counterintelligence as source-integrity defense: the class studies how institutions protect evidence, people, access, and judgment from deception and compromise. The sequence opens with **Financial due-diligence typology exercise using synthetic records and compliance boundaries**, **Hybrid-threat indicator review using sample scenarios and policy thresholds**, **Private Military Corporations as Intelligence: Hybrid-threat indicator review using sample scenarios and policy thresholds** and applies the **Dissemination-and-Marking Control Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 74; module overview Section 37; curriculum atlas Section 2.

Triangulation anchors. In module 25's topic-lessons section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

37.2.2.1 Lesson 1: Financial due-diligence typology exercise using synthetic records and compliance boundaries **Concept. Financial due-diligence typology exercise using synthetic records and compliance boundaries** studies non-state actors through organizational indicators, funding patterns, and open-source evidence with strict minimization.

Why it matters. Financial due-diligence typology exercise connects classroom vocabulary to Counterintelligence and Source-Integrity Defense practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Financial due-diligence typology exercise using synthetic records and compliance boundaries rests on [012, 2026]. The closest source to this row notes: It argues that although such groups lack the technical collection capabilities of states, they compensate through open-source and human-source methods and benefit defensively from compartmentalized, cell-based structures and ideological cohesion. Use it for pinning down the scope of **Financial due-diligence typology exercise using synthetic records and compliance boundaries**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. Ground **Financial due-diligence typology exercise** in the evidence the row cites. [012, 2026] A Grey Dynamics analysis article (Rachel Brown, 2021) on how non-state actors conduct counterintelligence. It argues that although such groups lack the technical collection capabilities of states, they compensate through open-source and human-source methods and benefit defensively from compartmentalized, cell-based structures and ideological cohesion. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Financial due-diligence typology exercise**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this deception-aware source review and defensive escalation topic. The artifact must note the typology descriptor, the bounded claim about **Financial due-diligence typology exercise using**, the intent caveat, the uncertainty threshold, the no-accusation boundary, and the reviewer who owns escalation. Shape **Financial due-diligence typology exercise** work as an **ambiguous-threshold indicator matrix** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Financial due-diligence typology exercise**: that a typology or pattern match is proof of intent rather than a flag requiring corroboration and alternative explanations.

Transfer task. Apply this module's safe boundary for **Financial due-diligence typology exercise** to another artifact while keeping deception-aware source review and defensive escalation and reviewer ownership explicit.

37.2.2.2 Lesson 2: Hybrid-threat indicator review using sample scenarios and policy thresholds **Concept. Hybrid-threat indicator review using sample scenarios and policy thresholds** identifies ambiguous-threshold activity through indicators, attribution caution, and policy review—not through prescribed response actions.

Why it matters. Hybrid-threat indicator review matters in the **Counterintelligence and Source-Integrity Defense** lane because deception-aware source review and defensive escalation evidence must stay separate from judgment; source compromise is a common failure.

Source support. Hybrid-threat indicator review using sample scenarios and policy thresholds rests on [308, 2026] and [311, 2026]. The lead source's own note reads: An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. Use them for pinning down the scope of **Hybrid-threat indicator review using sample scenarios and policy thresholds**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. Read **Hybrid-threat indicator review** against the works cited for this row. [308, 2026] An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure. [311, 2026] An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Hybrid-threat indicator review**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this deception-aware source review and defensive escalation topic. The artifact must name the indicator descriptor, the bounded claim about **Hybrid-threat indicator review using sample**, the attribution caveat, the threshold uncertainty, the non-attribution boundary, and the reviewer who approves the policy read. Shape **Hybrid-threat indicator review** work as an **ambiguous-threshold indicator matrix** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Hybrid-threat indicator review**: that activity falling below an obvious threshold is therefore ungoverned, rather than still bound by escalation limits and accountable review.

Transfer task. Transfer **Hybrid-threat indicator review** from this module to a second motif by preserving deception-aware source review and defensive escalation, replacing action with audit, and naming the blocked use.

37.2.2.3 Lesson 3: Private Military Corporations as Intelligence: Hybrid-threat indicator review using sample scenarios and policy thresholds **Concept. Private Military Corporations as Intelligence: Hybrid-threat indicator review using sample scenarios and policy thresholds** identifies ambiguous-threshold activity through indicators, attribution caution, and policy review—not through prescribed response actions.

Why it matters. Analysts use **Private Military Corporations as Intelligence** to separate defensive awareness from surveillance, handling, or operational security playbooks. A defensible treatment names the judgment it enables for deception-aware source review and defensive escalation review, the proof limit that source compromise would otherwise hide, and the reviewer accountable for challenge.

Source support. Private Military Corporations as Intelligence: Hybrid-threat indicator review using sample scenarios and policy thresholds rests on [308, 2026] and [311, 2026]. The lead source's own note reads: An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. Use them for the claim that **Private Military Corporations as Intelligence: Hybrid-threat indicator review using sample scenarios and policy thresholds** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. Ground **Private Military Corporations as Intelligence** in the evidence the row cites. [308, 2026] An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure. [311, 2026] An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Private Military Corporations as Intelligence**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this deception-aware source review and defensive escalation topic. The artifact must name the indicator descriptor, the bounded claim about **Private Military Corporations as Intelligence**, the attribution caveat, the threshold uncertainty, the non-attribution boundary, and the reviewer who approves the policy read. Shape **Private Military Corporations as Intelligence** work as an **ambiguous-threshold indicator matrix** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Private Military Corporations as Intelligence**: that activity falling below an obvious threshold is therefore ungoverned, rather than still bound by escalation limits and accountable review.

Transfer task. Reuse the **Private Military Corporations as Intelligence** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

37.2.2.4 Lesson 4: Non-state actor indicator review with attribution caution and governance boundaries

Concept. Non-state actor indicator review with attribution caution and governance boundaries uses attribution indicators cautiously by separating technical similarity, context, confidence, and geopolitical inference.

Why it matters. Analysts use **Non-state actor indicator review** to separate defensive awareness from surveillance, handling, or operational security playbooks. A defensible treatment names the judgment it enables for deception-aware source review and defensive escalation review, the proof limit that source compromise would otherwise hide, and the reviewer accountable for challenge.

Source support. Non-state actor indicator review with attribution caution and governance boundaries rests on [033, 2026]. The lead source's own note reads: How seriously is the U.S. Use it for the claim that **Non-state actor indicator review with attribution caution and governance boundaries** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. For **Non-state actor indicator review**, work from the cited evidence behind this row. [033, 2026] How seriously is the U.S. Intelligence Community (IC) considering this challenge to U.S. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Non-state actor indicator review**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this deception-aware source review and defensive escalation topic. The artifact must name the actor descriptor, the bounded claim about **state actor indicator review with**, the attribution caveat, the uncertainty note, the non-targeting boundary, and the reviewer who approves the assessment. Shape **Non-state actor indicator review** work as an **ambiguous-threshold indicator matrix** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that lacking a state sponsor places an actor outside the reach of governance, accountability, and applicable rules.

Transfer task. Reuse the **Non-state actor indicator review** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

37.2.2.5 Lesson 5: State Actor Use of Commercial: Non-state actor indicator review with attribution caution and governance boundaries

Concept. State Actor Use of Commercial: Non-state actor indicator review with attribution caution and governance boundaries uses attribution indicators cautiously by separating technical similarity, context, confidence, and geopolitical inference.

Why it matters. Without explicit treatment of **State Actor Use of Commercial**, source compromise undermines deception-aware source review and defensive escalation review; the lesson builds the habit to separate defensive awareness from surveillance, handling, or operational security playbooks.

Source support. State Actor Use of Commercial: Non-state actor indicator review with attribution caution and governance boundaries rests on [309, 2026], [310, 2026], and [300, 2026]. The most specific cited work observes: It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). Use them for the claim that **State Actor Use of Commercial: Non-state actor indicator review with attribution caution and governance boundaries** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. Ground **State Actor Use of Commercial** in the evidence the row cites. [309, 2026] An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection. [310, 2026] The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **State Actor Use of Commercial**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this deception-aware source review and defensive escalation topic. The artifact must name the actor descriptor, the bounded claim about **State Actor Use of Commercial**, the attribution caveat, the uncertainty note, the non-targeting boundary, and the reviewer who approves the assessment. Shape **State Actor Use of Commercial** work as an **ambiguous-threshold indicator matrix** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that lacking a state sponsor places an actor outside the reach of governance, accountability, and applicable rules.

Transfer task. Reuse the **State Actor Use of Commercial** audit pattern from this module on a different sample record set with a new reviewer

and blocked-use note.

37.2.3 Non-State Actor Intelligence worked safe example: synthetic inputs, evidence, and review

Worked example: a sample research lab reviews a synthetic source-quality anomaly after a disputed report. [238, 2026]; [247, 2026].

Triangulation anchors. In module 25's worked-example section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **hybrid-threat governance**. Learners use a **ambiguous-threshold indicator matrix** and keep this boundary visible: No live targeting, covert action, retaliation planning, or attribution certainty beyond evidence.

Frame. The classroom question centers on **Financial due-diligence typology exercise using synthetic records and compliance boundaries**. Excluded actions stay explicit, and the **Dissemination-and-Marking Control Lens** planning question is: Which audience, release authority, marking vocabulary, records duty, and feedback loop governs this intelligence artifact?

Inputs. For the **Financial due-diligence typology exercise using synthetic records and compliance boundaries** scenario, use toy access logs, public policy excerpts, synthetic source notes, and a reviewer escalation path. The Dissemination-and-Marking Control Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Financial due-diligence typology exercise using synthetic records and compliance boundaries**, students separate identity from access, list anomaly hypotheses, seek corroboration, and route sensitive concerns to review. Pause whenever an inference about Financial due-diligence typology exercise using synthetic records and compliance boundaries appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Financial due-diligence typology exercise using synthetic records and compliance boundaries** classroom scenario; unit artifact = ambiguous-threshold indicator matrix; evidence = allowed inputs; method = deception-aware source review and defensive escalation; output = a source-integrity memo with competing explanations, confidence, protected-disclosure note, and next-review owner; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Financial due-diligence typology exercise using synthetic records and compliance boundaries** as "Dissemination-and-Marking Control Lens confirms it" is not enough. The revision ties the claim to deception-aware source review and defensive escalation, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Financial due-diligence typology exercise using synthetic records and compliance boundaries** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

37.2.4 Non-State Actor Intelligence practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Dissemination-and-Marking Control Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**.

Triangulation anchors. In module 25's practice-sequence section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Financial due-diligence typology exercise using synthetic records and compliance boundaries, Hybrid-threat indicator review using sample scenarios and policy thresholds, Private Military Corporations as Intelligence: Hybrid-threat indicator review using sample scenarios and policy thresholds; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Counterintelligence and Source-Integrity Defense** lane.
2. Frame	Answer the lens question: Which audience, release authority, marking vocabulary, records duty, and feedback loop governs this intelligence artifact?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Financial due-diligence typology exercise using synthetic records and compliance boundaries: dissemination map with audience, caveat, marking, records, and feedback fields.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the ambiguous-threshold indicator matrix fields for Financial due-diligence typology exercise using synthetic records and compliance boundaries.	Unit profile note.	Evidence artifacts include threshold indicator, attribution caveat.
4. Challenge	Test the misconception that a typology or pattern match is proof of intent rather than a flag requiring corroboration and alternative explanations.	Failure-mode note.	The artifact applies the key distinction: separate defensive awareness from surveillance, handling, or operational security playbooks.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

37.2.4.1 Non-State Actor Intelligence instructor notes: source reasoning, review points, and studio focus Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**. [238, 2026]; [247, 2026].

37.2.4.2 Non-State Actor Intelligence extension exercise: peer validation and refresh trigger review **Evidence anchor.** Section 37; [238, 2026].

Have learners swap artifacts and apply the **Dissemination-and-Marking Control Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**.

37.2.5 Non-State Actor Intelligence knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 37; [238, 2026].

1. Explain how **Financial due-diligence typology exercise using synthetic records and compliance boundaries** is defined here; name the source descriptor that supports the definition.
2. Contrast **Financial due-diligence typology exercise using synthetic records and compliance boundaries** with **Hybrid-threat indicator review using sample scenarios and policy thresholds** using the **Dissemination-and-Marking Control Lens** artifact fields.
3. Identify one failure mode from the **Counterintelligence and Source-Integrity Defense** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which explanation preserves uncertainty without ignoring a possible compromise signal?
5. Correct this misconception: that a typology or pattern match is proof of intent rather than a flag requiring corroboration and alternative explanations.

37.2.5.1 Non-State Actor Intelligence answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Financial due-diligence typology exercise using synthetic records and compliance boundaries** without source evidence, uncertainty, or a safe transfer task.

37.3 Non-State Actor Intelligence assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 37; [238, 2026].

37.3.1 Non-State Actor Intelligence evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 37; [238, 2026].

37.3.2 Non-State Actor Intelligence transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 37; [238, 2026].

37.3.2.1 Non-State Actor Intelligence lineage and source tradition: profile, concepts, and first anchors This sits in the **Counterintelligence and Source-Integrity Defense** lineage: defending institutions, sources, and judgments against deception, insider risk, foreign-intelligence targeting, and source contamination. [238, 2026]; [247, 2026].

37.3.2.2 Non-State Actor Intelligence working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 37; [238, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**, with provenance and reviewability throughout.

37.3.2.3 Non-State Actor Intelligence knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [238, 2026]; [247, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

37.3.2.4 Non-State Actor Intelligence transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 37; [238, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**.
- **Evidence contract:** keep the **Counterintelligence and Source-Integrity Defense** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

37.3.2.5 Non-State Actor Intelligence profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 37; [238, 2026].

The matched profile emphasizes defending institutions, sources, and judgments against deception, insider risk, foreign-intelligence targeting, and source contamination. The method stack is threat awareness, source-descriptor audit, corroboration, anomaly review, red-team challenge, and protected disclosure paths; the local topic cluster is **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**.

37.3.3 Non-State Actor Intelligence evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 37; [238, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Counterintelligence and Source-Integrity Defense** profile tells reviewers what evidence is strong enough for the module artifact built around **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**.

37.3.3.1 Non-State Actor Intelligence guide source spine: inherited keys and local citation roles Primary guide citations: [238, 2026]; [247, 2026]; [249, 2026]; [273, 2026]; [274, 2026]; [275, 2026]; [286, 2026]; [287, 2026]; [292, 2026]; [012, 2026]; [033, 2026]; [308, 2026]; [311, 2026]; [309, 2026]; [310, 2026]; [300, 2026].

37.3.3.2 Non-State Actor Intelligence verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [238, 2026]; [247, 2026].

Tier	What counts	How it is used
Source guide	[238, 2026]; [247, 2026]; [249, 2026]; [273, 2026]; [274, 2026]; [275, 2026]; [286, 2026]; [287, 2026]; [292, 2026]; [012, 2026]; [033, 2026]; [308, 2026]; [311, 2026]; [309, 2026]; [310, 2026]; [300, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 25's source-canon section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds** and [238, 2026]; [247, 2026], but only directly verified source URLs are encoded as citations.

37.3.3.3 Non-State Actor Intelligence intelligence practice lens: evidence artifact and safety check Practice lens: **Dissemination-and-Marking Control Lens** for **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**. [238, 2026]; [247, 2026].

Planning question: Which audience, release authority, marking vocabulary, records duty, and feedback loop governs this intelligence artifact?

Evidence artifact: dissemination map with audience, caveat, marking, records, and feedback fields.

Validation rule: verify source authority, public/classification status, CAPCO-safe vocabulary, audience need, and records disposition before reuse. Applied to **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**.

Handoff contract: deliver release-neutral summaries, source metadata, marking rationale, and review ownership as separate fields.

Safety check: exclude classified content, live release decisions, source-method exposure, and improvised control markings.

37.3.3.4 Non-State Actor Intelligence runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 37; [238, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	25.99	25.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Non-State Actor Intelligence to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Bounded autonomy, procurement, incident-response, and assurance studio	25.101	25.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Non-State Actor Intelligence	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Model-card, recoverability, retention, and learner-support evidence package	25.102	25.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Non-State Actor Intelligence	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Financial due-diligence typology exercise using synthetic records and compliance boundaries	25.1	25.1 source title transformed into safe curriculum treatment; original: Typology: Terrorist, Criminal, Commercial, Hacktivist, Proxy	Economic-Security Due-Diligence Lens	economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary	exclude sanctions evasion, laundering methods, threshold gaming, procurement bypasses, and tailored targeting of real firms

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Hybrid-threat indicator review using sample scenarios and policy thresholds	25.2	25.2 source title transformed into safe curriculum treatment; original: Hezbollah, ISIS, MS-13: Intelligence Structures and Capabilities	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Hybrid-threat indicator review using sample scenarios and policy thresholds	25.3	25.3 source title transformed into safe curriculum treatment; original: Private Military Corporations as Intelligence Actors	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Non-state actor indicator review with attribution caution and governance boundaries	25.4	25.4 source title transformed into safe curriculum treatment; original: Counterintelligence Threat from Non-State Actors	AI/Data Accountability Lens	AI/data impact card with authority, provenance, model version, impact score, register status, human owner, and review cadence	reject automated adverse action, hidden surveillance expansion, unowned outputs, unreviewed model drift, and opaque downstream reuse
Non-state actor indicator review with attribution caution and governance boundaries	25.5	25.5 source title transformed into safe curriculum treatment; original: Non-State Actor Use of Commercial AI for Intelligence Collection	AI/Data Accountability Lens	AI/data impact card with authority, provenance, model version, impact score, register status, human owner, and review cadence	reject automated adverse action, hidden surveillance expansion, unowned outputs, unreviewed model drift, and opaque downstream reuse

37.3.3.5 Non-State Actor Intelligence reusable subsection contract: topic rows, artifacts, and safety duties Evidence anchor. Section 37; [238, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Financial due-diligence typology exercise using synthetic records and compliance boundaries	Economic-Security Due-Diligence Lens	economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary	exclude sanctions evasion, laundering methods, threshold gaming, procurement bypasses, and tailored targeting of real firms
Hybrid-threat indicator review using sample scenarios and policy thresholds	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Private Military Corporations as Intelligence: Hybrid-threat indicator review using sample scenarios and policy thresholds	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Non-state actor indicator review with attribution caution and governance boundaries	AI/Data Accountability Lens	AI/data impact card with authority, provenance, model version, impact score, register status, human owner, and review cadence	reject automated adverse action, hidden surveillance expansion, unowned outputs, unreviewed model drift, and opaque downstream reuse
State Actor Use of Commercial: Non-state actor indicator review with attribution caution and governance boundaries	AI/Data Accountability Lens	AI/data impact card with authority, provenance, model version, impact score, register status, human owner, and review cadence	reject automated adverse action, hidden surveillance expansion, unowned outputs, unreviewed model drift, and opaque downstream reuse

37.3.3.6 Non-State Actor Intelligence annotated source ledger: real titles and local contribution Each source cited by this **Counterintelligence and Source-Integrity Defense** module is paired below with its real title and a one-line note on what it contributes to **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**.

Source	Cited work	What it contributes	Status
[238, 2026]	Recommendation on the Ethics of Artificial Intelligence	The official UNESCO page for the Recommendation on the Ethics of Artificial Intelligence, the first global standard-setting instrument on AI ethics, adopted in 2021 and applicable to all 194 member states. It outlines four core values, including human rights protection and environmental flourishing, and ten guiding principles such as proportionality, privacy, transparency, and fairness.	verified source-guide

Source	Cited work	What it contributes	Status
[247, 2026]	AI in the Public Sector	Official OECD.AI public-sector AI theme page.	original source-guide
[249, 2026]	GovTech: Putting People First	The official page for the World Bank's Global Program on GovTech and Public Sector Innovation, which helps governments use technology and data to improve public services and governance. It describes support for digital transformation in public administration across areas such as tax administration, public financial management, human resource systems, and citizen engagement, with cross-cutting themes including responsible AI and green digital transformation.	verified source-guide
[273, 2026]	WCAG 2 Overview	The W3C Web Accessibility Initiative overview of the Web Content Accessibility Guidelines (WCAG), an international standard for making web content accessible to people with disabilities. It explains that WCAG is organized around four principles (perceivable, operable, understandable, robust) with testable success criteria at three conformance levels (A, AA, AAA), and covers versions 2.0, 2.1, and 2.2.	verified source-guide
[274, 2026]	CAST Universal Design for Learning Guidelines version 3.0	The official CAST website for the Universal Design for Learning (UDL) Guidelines version 3.0, released in 2024. The framework offers research-based guidance for designing inclusive learning environments and is organized around three principles: Engagement (motivation and emotional support), Representation (accessible presentation of information), and Action and Expression (diverse means of participation and communication).	verified source-guide
[275, 2026]	Fact Sheet: New Rule on the Accessibility of Web Content and Mobile Apps Provided by State and Local Governments	A US Department of Justice fact sheet explaining the 2024 ADA Title II rule requiring state and local governments to make their web content and mobile apps accessible. It establishes WCAG 2.1 Level AA as the technical standard, applies to entities such as schools, courts, libraries, and transit agencies, and sets compliance deadlines of April 2027 for larger jurisdictions and April 2028 for smaller ones.	verified source-guide
[286, 2026]	Model Cards for Model Reporting	The arXiv abstract for "Model Cards for Model Reporting" (2018) by Mitchell, Wu, Zaldivar, and colleagues, which introduces a framework for transparent documentation of machine learning models. Model cards are short accompanying documents that report a model's benchmarked performance across varied conditions, including different cultural, demographic, and phenotypic groups, along with intended use, evaluation methodology, and deployment considerations.	verified source-guide

Source	Cited work	What it contributes	Status
[287, 2026]	Datasheets for Datasets	A 2018 arXiv paper proposing 'datasheets for datasets,' a standardized documentation framework for machine learning datasets modeled on electronic component datasheets. The authors argue the field lacks consistent dataset documentation, which creates risk in high-stakes applications, and propose that datasets be accompanied by documentation covering motivation, composition, collection process, recommended uses, and test results.	verified source-guide
[292, 2026]	Assessing Risks and Impacts of AI (ARIA): Pilot Evaluation Report	The ARIA 0.1 pilot evaluation report documents NIST's methodology for systematically assessing AI applications for risks and societal impacts, using a multi-layered evaluation approach across five participating organizations and seven submitted AI applications. The pilot employed three evaluation scenarios and three testing levels: model testing, red teaming, and field testing, supplemented by dialogue annotation, tester questionnaires, and structured measurement trees.	verified source-guide
[012, 2026]	Counterintelligence Activities of Non-State Actors - Grey Dynamics	A Grey Dynamics analysis article (Rachel Brown, 2021) on how non-state actors conduct counterintelligence. It argues that although such groups lack the technical collection capabilities of states, they compensate through open-source and human-source methods and benefit defensively from compartmentalized, cell-based structures and ideological cohesion.	verified source-guide
[033, 2026]	The Counterintelligence Threat from Non-State Actors	How seriously is the U.S. Intelligence Community (IC) considering this challenge to U.S.	original source-guide context; do not use as primary analytic support
[308, 2026]	Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure	An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure.	verified source-guide
[311, 2026]	Countering Information Threats	An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering.	verified source-guide
[309, 2026]	STIX Version 2.1	An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection.	verified source-guide

Source	Cited work	What it contributes	Status
[310, 2026]	TAXII Version 2.1	The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe).	verified source-guide
[300, 2026]	MITRE ATLAS	MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy.	original source-guide

Where this sits. This module's overview is Section 37; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

37.3.4 Non-State Actor Intelligence governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 37; [238, 2026].

37.3.5 Non-State Actor Intelligence analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 25's governance-boundary section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **Counterintelligence and Source-Integrity Defense** for **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**. [238, 2026]; [247, 2026].

Curriculum topic spine: Financial due-diligence typology exercise using synthetic records and compliance boundaries, **Hybrid-threat indicator review using sample scenarios and policy thresholds**, **Private Military Corporations as Intelligence: Hybrid-threat indicator review using sample scenarios and policy thresholds**. **Verified anchor cluster:** [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]; [Agency, 2009]; [Jr., 2007]; [Burkett, 2013].

Conceptual depth: defending institutions, sources, and judgments against deception, insider risk, foreign-intelligence targeting, and source contamination.

Method stack: threat awareness, source-descriptor audit, corroboration, anomaly review, red-team challenge, and protected disclosure paths.

Composability contract: identity, access, reporting, corroboration, caveats, and confidence are modeled independently so defensive review can happen without exposure.

Known failure modes: source compromise, deception acceptance, identity overconfidence, insider blind spots, and collapsing CI concerns into undifferentiated IT-security triage.

Defensive boundary: CI content supports defensive awareness, source protection, and analytic integrity; it does not provide surveillance or handling playbooks. Applied to **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**.

Anchor	Why it matters here
[Counterintelligence and Center, 2024]	Official strategy for defensive CI integration, foreign-intelligence threat awareness, strategic advantage protection, and future readiness. Checked as of 2026-05-21; role: curriculum_anchor.
[Archives and Administration, 1981]	Official legal anchor for intelligence authorities, rights-aware collection, analytic competition, oversight, and source-method protection. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026d]	Official sourcing directive for traceability, citations, source descriptors, and source summaries. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2015]	Official ODNI analytic tradecraft standards directive. Checked as of 2026-05-21; role: source_quality_anchor.
[Agency, 2009]	Official structured analytic techniques primer for bias checks, alternatives, and warning analysis. Checked as of 2026-05-21; role: curriculum_anchor.
[Jr., 2007]	Foundational analytic cognition source for bias, mental models, and structured reasoning. Checked as of 2026-06-06; role: curriculum_anchor.
[Burkett, 2013]	A CIA Studies in Intelligence analyst essay arguing that the traditional MICE recruitment-motivation model (Money, Ideology, Compromise, Ego) is better understood through Cialdini's influence principles reframed as RASCLS (Reciprocation, Authority, Scarcity, Commitment/Consistency, Liking, Social Proof), grounding the historical and conceptual lineage of HUMINT recruitment frameworks. Checked as of 2026-06-08; role: curriculum_anchor.

37.3.5.1 Non-State Actor Intelligence evidence standard and citation floor: source families and discovery limits Official guidance supplies governance, safety, and legal constraints for the **Counterintelligence and Source-Integrity Defense** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [238, 2026]; [247, 2026].

37.3.6 Non-State Actor Intelligence agentic boundary: assist, approve, block, and record

Evidence anchor. Section 37; [238, 2026].

AGEINT translation is bounded by the **Counterintelligence and Source-Integrity Defense** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**.

37.3.6.1 Non-State Actor Intelligence permitted defensive utility: curriculum uses and safe outputs **Evidence anchor.** Section 37; [238, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**.

37.3.6.2 Non-State Actor Intelligence excluded operational boundary: blocked actions and stop rules Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [238, 2026]; [247, 2026] and **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

37.3.7 Non-State Actor Intelligence governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 37; [238, 2026].
Governance is practiced as a gate on the **Counterintelligence and Source-Integrity Defense** lane. Learners use the **Dissemination-and-Marking Control Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**.

37.3.7.1 Non-State Actor Intelligence governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [238, 2026]; [247, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Counterintelligence and Source-Integrity Defense** failure modes and the **Dissemination-and-Marking Control Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

37.3.7.2 Non-State Actor Intelligence evidence package handoff: appendices, records, and reuse

Evidence anchor. Section 37; [238, 2026].
Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Dissemination-and-Marking Control Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**.

37.3.7.3 Non-State Actor Intelligence current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**. [238, 2026]; [247, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_ncsc_counterintelligence_strategy` for **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**?	The National Counterintelligence Strategy; lane `counterintelligence_source_integrity`; checked 2026-05-21.	dissemination map with audience, caveat, marking, records, and feedback fields; Official strategy for defensive CI integration, foreign-intelligence threat awareness, strategic advantage protection, and future readiness.
What does the module inherit from `official_odni_eo_12333` for **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**?	Executive Order 12333: United States Intelligence Activities; lane `legal_oversight`; checked 2026-05-21.	dissemination map with audience, caveat, marking, records, and feedback fields; Official legal anchor for intelligence authorities, rights-aware collection, analytic competition, oversight, and source-method protection.
What does the module inherit from `official_odni_icd_206` for **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**?	Intelligence Community Directive 206: Sourcing Requirements for Disseminated Analytic Products; lane `analytic_tradecraft`; checked 2026-05-21.	dissemination map with audience, caveat, marking, records, and feedback fields; Official sourcing directive for traceability, citations, source descriptors, and source summaries.
What does the module inherit from `official_odni_icd_203` for **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**?	Intelligence Community Directive 203: Analytic Standards; lane `source_quality_spine`; checked 2026-05-21.	dissemination map with audience, caveat, marking, records, and feedback fields; Official ODNI analytic tradecraft standards directive.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 37; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

37.3.8 Non-State Actor Intelligence assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 37; [238, 2026].

37.3.9 Non-State Actor Intelligence assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 37; [238, 2026].

37.3.9.1 Non-State Actor Intelligence capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds** and [238, 2026]; [247, 2026].

37.3.9.2 Non-State Actor Intelligence instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds** and [238, 2026]; [247, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

37.3.9.3 Non-State Actor Intelligence assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Financial due-diligence typology exercise using synthetic records and compliance boundaries	Completed **dissemination map with audience, caveat, marking, records, and feedback fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Hybrid-threat indicator review using sample scenarios and policy thresholds	Completed **dissemination map with audience, caveat, marking, records, and feedback fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Private Military Corporations as Intelligence: Hybrid-threat indicator review using sample scenarios and policy thresholds	Completed **dissemination map with audience, caveat, marking, records, and feedback fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

37.3.10 Non-State Actor Intelligence refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [238, 2026]; [247, 2026] and **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**.

37.3.10.1 Non-State Actor Intelligence refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**. The local signals begin with [238, 2026]; [247, 2026].

37.3.10.2 Non-State Actor Intelligence claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**, and the source spine for these checks begins with [238, 2026]; [247, 2026].

37.3.11 Non-State Actor Intelligence reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [238, 2026]; [247, 2026].

Triangulation anchors. In module 25's review-checklist section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds**. [238, 2026]; [247, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.

- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

37.3.12 Non-State Actor Intelligence learning-path links: module map, overview, and curriculum atlas

These links keep **Financial due-diligence typology exercise using synthetic records and compliance boundaries; Hybrid-threat indicator review using sample scenarios and policy thresholds** paired with the orientation atlas, the parent unit, and the previous and next modules, so a reader can trace which claims and caveats are inherited rather than re-derived here. Anchored at [238, 2026]; [247, 2026].
Section 2, Section 35, Section 36, Section 38

38 Irregular Warfare and Special Operations

38.0.1 Irregular Warfare and Special Operations figures and course links: visual evidence, source flow, and navigation

The module uses Figure 78 and Figure 74 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.

Navigation links: Section 2, Section 35, Section 37, Section 39.

This module teaches the **Counterintelligence and Source-Integrity Defense** lane through a bounded, source-backed coursebook chapter. [239, 2026]; [249, 2026].

38.1 Counterintelligence and Source-Integrity Defense frame for Irregular Warfare and Special Operations: source context, topic focus, and reader task

Evidence anchor. Section 38; [239, 2026].

38.1.1 Irregular Warfare and Special Operations orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 38; [239, 2026].

38.1.2 Irregular Warfare and Special Operations conceptual primer: source context, core model, and reader task

This chapter teaches counterintelligence as source-integrity defense: the class studies how institutions protect evidence, people, access, and judgment from deception and compromise. The chapter uses **Dissemination-and-Marking Control Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**.

The central distinction is to separate defensive awareness from surveillance, handling, or operational security playbooks. Core topics include **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 102: Hybrid-threat indicator review using sample scenarios and policy thresholds**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.

Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [239, 2026]; [249, 2026].

Learners move from vocabulary and the **Dissemination-and-Marking Control Lens** distinction through topic lessons on **Hybrid-threat indicator review using sample scenarios and policy thresholds** with evidence and misconception checks, then assemble a **dissemination map with audience, caveat, marking, records, and feedback fields** with safety and rights gates.

38.1.3 Irregular Warfare and Special Operations learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 38; [239, 2026].

- Connect **Hybrid-threat indicator review using sample scenarios and policy thresholds and FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds** to **Counterintelligence and Source-Integrity Defense** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **dissemination map with audience, caveat, marking, records, and feedback fields** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate defensive awareness from surveillance, handling, or operational security playbooks; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as source compromise, deception acceptance, identity overconfidence, insider blind spots, and collapsing CI concerns into undifferentiated IT-security triage, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: CI content supports defensive awareness, source protection, and analytic integrity; it does not provide surveillance or handling playbooks.

38.1.4 Irregular Warfare and Special Operations core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 38; [239, 2026].

Term	Working definition
Source integrity	confidence that evidence has not been distorted, laundered, or compromised
Compromise signal	a clue that access, identity, or source reliability needs review
Corroboration	independent support that reduces single-source vulnerability
Insider risk	risk created by trusted access combined with motive, pressure, or control failure
Protected disclosure	a safe channel for reporting concerns without exposing sensitive details
Hybrid-threat indicator review using sample…	Key terms: Hybrid, threat, indicator.
FM 3-05 130: Hybrid-threat indicator review…	Key terms: FM, Hybrid, threat.

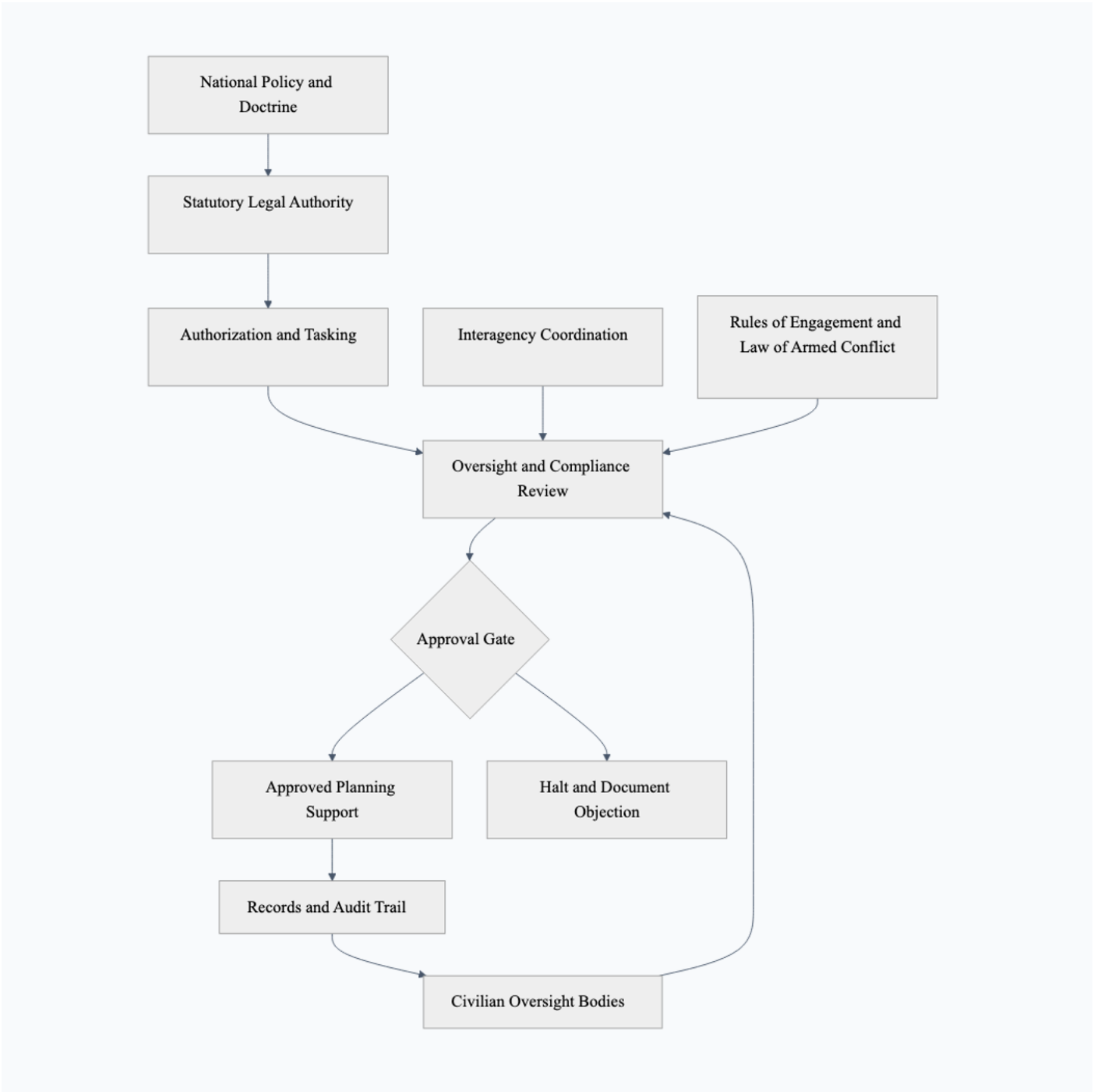


Figure 78: How intelligence support to special operations flows only through documented legal authority, oversight review, and approval gates before any approved planning proceeds. The captioned view belongs to the gray zone hybrid warfare and non state actors / irregular warfare and special operations section and should be read as a map of National Policy and Doctrine, Statutory Legal Authority, Authorization and Tasking, and Oversight and Compliance Review, not as a capability score or live-task instruction.

38.2 Dissemination-and-Marking Control Lens path for Irregular Warfare and Special Operations: lesson cluster, safe artifact, and review

Evidence anchor. Section 38; [239, 2026].

38.2.1 Irregular Warfare and Special Operations practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 38; [239, 2026].

38.2.2 Irregular Warfare and Special Operations topic lessons: source-backed concepts and transfer tasks

This module builds counterintelligence as source-integrity defense: the class studies how institutions protect evidence, people, access, and judgment from deception and compromise. The sequence opens with **Hybrid-threat indicator review using sample scenarios and policy thresholds**, **FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**, **FM 3-05 102: Hybrid-threat indicator review using sample scenarios and policy thresholds** and applies the **Dissemination-and-Marking Control Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 74; module overview Section 38; curriculum atlas Section 2.

Triangulation anchors. In module 26's topic-lessons section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

38.2.2.1 Lesson 1: Hybrid-threat indicator review using sample scenarios and policy thresholds **Concept. Hybrid-threat indicator review using sample scenarios and policy thresholds** reads special-operations intelligence as support to accountable planning with explicit authority and oversight fields.

Why it matters. Analysts use **Hybrid-threat indicator review** to separate defensive awareness from surveillance, handling, or operational security playbooks. A defensible treatment names the judgment it enables for deception-aware source review and defensive escalation review, the proof limit that source compromise would otherwise hide, and the reviewer accountable for challenge.

Source support. Hybrid-threat indicator review using sample scenarios and policy thresholds rests on [112, 2026]. The closest source to this row notes: It presents a seven-phase operational framework encompassing psychological preparation, infiltration, organization of underground and guerrilla forces, employment, and transition. Use it for pinning down the scope of **Hybrid-threat indicator review using sample scenarios and policy thresholds**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. For **Hybrid-threat indicator review**, work from the cited evidence behind this row. [112, 2026] This U.S. Army Training Circular (TC 18-01) defines the Special Forces concept for planning and conducting unconventional warfare operations, covering how units enable and support resistance movements in denied or hostile territory. It presents a seven-phase operational framework encompassing psychological preparation, infiltration, organization of underground and guerrilla forces, employment, and transition. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Hybrid-threat indicator review**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this deception-aware source review and defensive escalation topic. The artifact must name the indicator descriptor, the bounded claim about **Hybrid-threat indicator review using sample**, the attribution caveat, the threshold uncertainty, the non-attribution boundary, and the reviewer who approves the policy read. Shape **Hybrid-threat indicator review** work as an **ambiguous-threshold indicator matrix** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Hybrid-threat indicator review**: that activity falling below an obvious threshold is therefore ungoverned, rather than still bound by escalation limits and accountable review.

Transfer task. Transfer **Hybrid-threat indicator review** from this module to a second motif by preserving deception-aware source review and defensive escalation, replacing action with audit, and naming the blocked use.

38.2.2.2 Lesson 2: FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds **Concept. FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds** reads special-operations intelligence as support to accountable planning with explicit authority and oversight fields.

Why it matters. FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds matters in the **Counter-intelligence and Source-Integrity Defense** lane because deception-aware source review and defensive escalation evidence must stay separate from judgment; source compromise is a common failure.

Source support. FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds rests on [113, 2026] and [114, 2026]. The most specific cited work observes: Distribution was restricted to U.S. Use them for the claim that **FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. Read **FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds** against the works cited for this row. [113, 2026] U.S. Army Field Manual FM 3-05.130, "Army Special Operations Forces Unconventional Warfare," published by Headquarters, Department of the Army in September 2008. The manual is organized into chapters covering an introduction to warfare types, the instruments of United States national power, national policy and doctrine, and planning considerations including the seven phases of unconventional warfare and the role of Army Special Operations Forces. [114, 2026] FM 3-05.130, Army Special Operations Forces Unconventional Warfare (Headquarters, Department of the Army, 30 September 2008). The manual defines unconventional warfare and situates it within U.S. national power, covering the seven phases of UW operations, Special Forces missions, psychological operations, civil affairs operations in the UW context, and the roles of supporting elements including interagency partners. Distribution was restricted to U.S. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **FM 3-05 130**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this deception-aware source review and defensive escalation topic. The artifact must name the indicator descriptor, the bounded claim about **FM 3-05 130**, the attribution caveat, the threshold uncertainty, the non-attribution boundary, and the reviewer who approves the policy read. Shape **FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds** work as an **ambiguous-threshold indicator matrix** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**: that activity falling below an obvious threshold is therefore ungoverned, rather than still bound by escalation limits and accountable review.

Transfer task. Apply this module's safe boundary for **FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds** to another artifact while keeping deception-aware source review and defensive escalation and reviewer ownership explicit.

38.2.2.3 Lesson 3: FM 3-05 102: Hybrid-threat indicator review using sample scenarios and policy thresholds Concept. FM 3-05 102: Hybrid-threat indicator review using sample scenarios and policy thresholds identifies ambiguous-threshold activity through indicators, attribution caution, and policy review—not through prescribed response actions.

Why it matters. Analysts use **FM 3-05 102: Hybrid-threat indicator review using sample scenarios and policy thresholds** to separate defensive awareness from surveillance, handling, or operational security playbooks. A defensible treatment names the judgment it enables for deception-aware source review and defensive escalation review, the proof limit that source compromise would otherwise hide, and the reviewer accountable for challenge.

Source support. FM 3-05 102: Hybrid-threat indicator review using sample scenarios and policy thresholds rests on [115, 2026] and [116, 2026]. The lead source's own note reads: A U.S. Use them for the working definition that **FM 3-05 102: Hybrid-threat indicator review using sample scenarios and policy thresholds** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. Ground **FM 3-05 102: Hybrid-threat indicator review using sample scenarios and policy thresholds** in the evidence the row cites. [115, 2026] FM 3-05.102, Army Special Operations Forces Intelligence (Headquarters, Department of the Army). The manual addresses intelligence and electronic warfare (IEW) support across Army Special Operations Force components, covering Special Forces, Rangers, ARSOA, PSYOP, and Civil Affairs operations. [116, 2026] A U.S. Army field manual, FM 3-05.102 (Army Special Operations Forces Intelligence), dated 2001 and superseding FM 34-36, distributed with restrictions to U.S. government agencies. The manual gives special operations forces commanders and staff a doctrinal overview of intelligence support to their missions, covering force structure, training, and operational requirements consistent with joint doctrine. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **FM 3-05 102**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this deception-aware source review and defensive escalation topic. The artifact must name the indicator descriptor, the bounded claim about **FM 3-05 102**, the attribution caveat, the threshold uncertainty, the non-attribution boundary, and the reviewer who approves the policy read. Shape **FM 3-05 102: Hybrid-threat indicator review using sample scenarios and policy thresholds** work as an **ambiguous-threshold indicator matrix** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **FM 3-05 102: Hybrid-threat indicator review using sample scenarios and policy thresholds**: that activity falling below an obvious threshold is therefore ungoverned, rather than still bound by escalation limits and accountable review.

Transfer task. Apply this module's safe boundary for **FM 3-05 102: Hybrid-threat indicator review using sample scenarios and policy thresholds** to another artifact while keeping deception-aware source review and defensive escalation and reviewer ownership explicit.

38.2.2.4 Lesson 4: Declassified training-manual archive Concept. Declassified training-manual archive studies OSS declassified manuals for oversight, ethics, and limits on translating history into practice.

Why it matters. Declassified training-manual archive connects classroom vocabulary to Counterintelligence and Source-Integrity Defense practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Declassified training-manual archive rests on [117, 2026], [118, 2026], and [119, 2026]. The closest source to this row notes: A digitized World War II field manual from the Internet Archive, the Special Operations Field Manual, Strategic Services (provisional), issued July 18, 1944 by the U.S. Use them for pinning down the scope of **Declassified training-manual archive**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. For **Declassified training-manual archive**, reason from the sources cited in this row. [117, 2026] An article from Small Wars Journal (affiliated with Arizona State University) announcing that The Resistance Hub has compiled declassified Office of Strategic Services (OSS) manuals for public access. The OSS was the WWII predecessor to the CIA, and the documents illustrate how the United States organized clandestine activities in occupied Europe and Asia. [118, 2026] A digitized World War II field manual from the Internet Archive, the Special Operations Field Manual, Strategic Services (provisional), issued July 18, 1944 by the U.S. Office of Strategic Services (OSS). The 32-page manual sets out the authorized functions, operational plans, methods, and organization of OSS Maritime Units and the broader Special Operations Branch. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. Build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this deception-aware source review and defensive escalation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **Declassified training-manual archive**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape this subject work as an **ambiguous-threshold indicator matrix** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Declassified training-manual archive**: that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Reuse the **Declassified training-manual archive** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

38.2.2.5 Lesson 5: Principles of Tradecraft for Resistance: Hybrid-threat indicator review using sample scenarios and policy thresholds Concept. Principles of Tradecraft for Resistance: Hybrid-threat indicator review using sample scenarios and policy thresholds identifies ambiguous-threshold activity through indicators, attribution caution, and policy review—not through prescribed response actions.

Why it matters. Principles of Tradecraft for Resistance connects classroom vocabulary to Counterintelligence and Source-Integrity Defense practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Principles of Tradecraft for Resistance: Hybrid-threat indicator review using sample scenarios and policy thresholds rests on [120, 2026]. The closest source to this row notes: The document presents an overview of intelligence and espionage concepts, with chapters covering an introduction to espionage, agents (typology, identification, recruitment, and handling), and agent organization and management including personnel and structures. Use it for pinning down the scope of **Principles of Tradecraft for Resistance: Hybrid-threat indicator review using sample scenarios and policy thresholds**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. Ground **Principles of Tradecraft for Resistance** in the evidence the row cites. [120, 2026] Principles of Tradecraft, a 1995 publication by Militia Free Press (a subsidiary of The Resister). The document presents an overview of intelligence and espionage concepts, with chapters covering an introduction to espionage, agents (typology, identification, recruitment, and handling), and agent organization and management including personnel and structures. It is framed as an introductory treatment rather than a comprehensive reference on intelligence requirements. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Principles of Tradecraft for Resistance**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this deception-aware source review and defensive escalation topic. The artifact must name the indicator descriptor, the bounded claim about **Principles of Tradecraft for Resistance**, the attribution caveat, the threshold uncertainty, the non-attribution boundary, and the reviewer who approves the policy read. Shape **Principles of Tradecraft for Resistance** work as an **ambiguous-threshold indicator matrix** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Principles of Tradecraft for Resistance**: that activity falling below an obvious threshold is therefore ungoverned, rather than still bound by escalation limits and accountable review.

Transfer task. Reuse the **Principles of Tradecraft for Resistance** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

38.2.2.6 Lesson 6: Underground Intelligence Networks: Hybrid-threat indicator review using sample scenarios and policy thresholds

Concept. Underground Intelligence Networks: Hybrid-threat indicator review using sample scenarios and policy thresholds identifies ambiguous-threshold activity through indicators, attribution caution, and policy review—not through prescribed response actions.

Why it matters. Underground Intelligence Networks connects classroom vocabulary to Counterintelligence and Source-Integrity Defense practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Underground Intelligence Networks: Hybrid-threat indicator review using sample scenarios and policy thresholds rests on [308, 2026] and [311, 2026]. The most specific cited work observes: An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. Use them for the working definition that **Underground Intelligence Networks: Hybrid-threat indicator review using sample scenarios and policy thresholds** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. For **Underground Intelligence Networks**, work from the cited evidence behind this row. [308, 2026] An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure. [311, 2026] An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Underground Intelligence Networks**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this deception-aware source review and defensive escalation topic. The artifact must name the indicator descriptor, the bounded claim about **Underground Intelligence Networks**, the attribution caveat, the threshold uncertainty, the non-attribution boundary, and the reviewer who approves the policy read. Shape **Underground Intelligence Networks** work as an **ambiguous-threshold indicator matrix** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Underground Intelligence Networks**: that activity falling below an obvious threshold is therefore ungoverned, rather than still bound by escalation limits and accountable review.

Transfer task. Transfer **Underground Intelligence Networks** from this module to a second motif by preserving deception-aware source review and defensive escalation, replacing action with audit, and naming the blocked use.

38.2.2.7 Lesson 7: OSS Simple Sabotage Field Manual: Hybrid-threat indicator review using sample scenarios and policy thresholds

Concept. OSS Simple Sabotage Field Manual: Hybrid-threat indicator review using sample scenarios and policy thresholds studies OSS declassified manuals for oversight, ethics, and limits on translating history into practice.

Why it matters. OSS Simple Sabotage Field Manual matters in the **Counterintelligence and Source-Integrity Defense** lane because deception-aware source review and defensive escalation evidence must stay separate from judgment; source compromise is a common failure.

Source support. OSS Simple Sabotage Field Manual: Hybrid-threat indicator review using sample scenarios and policy thresholds rests on [117, 2026]. Its anchor reference records: An article from Small Wars Journal (affiliated with Arizona State University) announcing that The Resistance Hub has compiled declassified Office of Strategic Services (OSS) manuals for public access. Use it for pinning down the scope of **OSS Simple Sabotage Field Manual: Hybrid-threat indicator review using sample scenarios and policy thresholds**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. For **OSS Simple Sabotage Field Manual**, reason from the sources cited in this row. [117, 2026] An article from Small Wars Journal (affiliated with Arizona State University) announcing that The Resistance Hub has compiled declassified Office of Strategic Services (OSS) manuals for public access. The OSS was the WWII predecessor to the CIA, and the documents illustrate how the United States organized clandestine activities in occupied Europe and Asia. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **OSS Simple Sabotage Field Manual**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this deception-aware source review and defensive escalation topic. The artifact must name the indicator descriptor, the bounded claim about **OSS Simple Sabotage Field Manual**, the attribution caveat, the threshold uncertainty, the non-attribution boundary, and the reviewer who approves the policy read. Shape **OSS Simple Sabotage Field Manual** work as an **ambiguous-threshold indicator matrix** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **OSS Simple Sabotage Field Manual**: that activity falling below an obvious threshold is therefore ungoverned, rather than still bound by escalation limits and accountable review.

Transfer task. Transfer **OSS Simple Sabotage Field Manual** from this module to a second motif by preserving deception-aware source review and defensive escalation, replacing action with audit, and naming the blocked use.

38.2.2.8 Lesson 8: Morale Operations: Hybrid-threat indicator review using sample scenarios and policy thresholds

Concept. Morale Operations: Hybrid-threat indicator review using sample scenarios and policy thresholds studies OSS declassified manuals for oversight, ethics, and limits on translating history into practice.

Why it matters. Morale Operations matters in the **Counterintelligence and Source-Integrity Defense** lane because deception-aware source review and defensive escalation evidence must stay separate from judgment; source compromise is a common failure.

Source support. Morale Operations: Hybrid-threat indicator review using sample scenarios and policy thresholds rests on [117, 2026]. Its anchor reference records: An article from Small Wars Journal (affiliated with Arizona State University) announcing that The Resistance Hub has compiled declassified Office of Strategic Services (OSS) manuals for public access. Use it for pinning down the scope of **Morale Operations: Hybrid-threat indicator review using sample scenarios and policy thresholds**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Counterintelligence and Center, 2024]; [Archives and Administration, 1981].

Evidence to inspect. For **Morale Operations**, work from the cited evidence behind this row. [117, 2026] An article from Small Wars Journal (affiliated with Arizona State University) announcing that The Resistance Hub has compiled declassified Office of Strategic Services (OSS) manuals for public access. The OSS was the WWII predecessor to the CIA, and the documents illustrate how the United States organized clandestine activities in occupied Europe and Asia. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Morale Operations**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this deception-aware source review and defensive escalation topic. The artifact must name the indicator descriptor, the bounded claim about **Morale Operations**, the attribution caveat, the threshold uncertainty, the non-attribution boundary, and the reviewer who approves the policy read. Shape **Morale Operations** work as an **ambiguous-threshold indicator matrix** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Morale Operations**: that activity falling below an obvious threshold is therefore ungoverned, rather than still bound by escalation limits and accountable review.

Transfer task. Reuse the **Morale Operations** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

38.2.3 Irregular Warfare and Special Operations worked safe example: synthetic inputs, evidence, and review

Worked example: a sample research lab reviews a synthetic source-quality anomaly after a disputed report. [239, 2026]; [249, 2026].

Triangulation anchors. In module 26's worked-example section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **hybrid-threat governance**. Learners use a **ambiguous-threshold indicator matrix** and keep this boundary visible: No live targeting, covert action, retaliation planning, or attribution certainty beyond evidence.

Frame. The classroom question centers on **Hybrid-threat indicator review using sample scenarios and policy thresholds**. Excluded actions stay explicit, and the **Dissemination-and-Marking Control Lens** planning question is: Which audience, release authority, marking vocabulary, records duty, and feedback loop governs this intelligence artifact?

Inputs. For the **Hybrid-threat indicator review using sample scenarios and policy thresholds** scenario, use toy access logs, public policy excerpts, synthetic source notes, and a reviewer escalation path. The Dissemination-and-Marking Control Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Hybrid-threat indicator review using sample scenarios and policy thresholds**, students separate identity from access, list anomaly hypotheses, seek corroboration, and route sensitive concerns to review. Pause whenever an inference about Hybrid-threat indicator review using sample scenarios and policy thresholds appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Hybrid-threat indicator review using sample scenarios and policy thresholds** classroom scenario; unit artifact = ambiguous-threshold indicator matrix; evidence = allowed inputs; method = deception-aware source review and defensive escalation; output = a source-integrity memo with competing explanations, confidence, protected-disclosure note, and next-review owner; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Hybrid-threat indicator review using sample scenarios and policy thresholds** as "Dissemination-and-Marking Control Lens confirms it" is not enough. The revision ties the claim to deception-aware source review and defensive escalation, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Hybrid-threat indicator review using sample scenarios and policy thresholds** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

38.2.4 Irregular Warfare and Special Operations practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Dissemination-and-Marking Control Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**.

Triangulation anchors. In module 26's practice-sequence section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Hybrid-threat indicator review using sample scenarios and policy thresholds, FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds, FM 3-05 102: Hybrid-threat indicator review using sample scenarios and policy thresholds; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Counterintelligence and Source-Integrity Defense** lane.
2. Frame	Answer the lens question: Which audience, release authority, marking vocabulary, records duty, and feedback loop governs this intelligence artifact?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Hybrid-threat indicator review using sample scenarios and policy thresholds: dissemination map with audience, caveat, marking, records, and feedback fields.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the ambiguous-threshold indicator matrix fields for Hybrid-threat indicator review using sample scenarios and policy thresholds.	Unit profile note.	Evidence artifacts include threshold indicator, attribution caveat.
4. Challenge	Test the misconception that activity falling below an obvious threshold is therefore ungoverned, rather than still bound by escalation limits and accountable review.	Failure-mode note.	The artifact applies the key distinction: separate defensive awareness from surveillance, handling, or operational security playbooks.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

38.2.4.1 Irregular Warfare and Special Operations instructor notes: source reasoning, review points, and studio focus Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor

or a human review point. Keep the focus on **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**. [239, 2026]; [249, 2026].

38.2.4.2 Irregular Warfare and Special Operations extension exercise: peer validation and refresh trigger review **Evidence anchor.** Section 38; [239, 2026].
Have learners swap artifacts and apply the **Dissemination-and-Marking Control Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**.

38.2.5 Irregular Warfare and Special Operations knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 38; [239, 2026].

1. Explain how **Hybrid-threat indicator review using sample scenarios and policy thresholds** is defined here; name the source descriptor that supports the definition.
2. Contrast **Hybrid-threat indicator review using sample scenarios and policy thresholds** with **FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds** using the **Dissemination-and-Marking Control Lens** artifact fields.
3. Identify one failure mode from the **Counterintelligence and Source-Integrity Defense** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which explanation preserves uncertainty without ignoring a possible compromise signal?
5. Correct this misconception: that activity falling below an obvious threshold is therefore ungoverned, rather than still bound by escalation limits and accountable review.

38.2.5.1 Irregular Warfare and Special Operations answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Hybrid-threat indicator review using sample scenarios and policy thresholds** without source evidence, uncertainty, or a safe transfer task.

38.3 Irregular Warfare and Special Operations assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 38; [239, 2026].

38.3.1 Irregular Warfare and Special Operations evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 38; [239, 2026].

38.3.2 Irregular Warfare and Special Operations transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 38; [239, 2026].

38.3.2.1 Irregular Warfare and Special Operations lineage and source tradition: profile, concepts, and first anchors This sits in the **Counterintelligence and Source-Integrity Defense** lineage: defending institutions, sources, and judgments against deception, insider risk, foreign-intelligence targeting, and source contamination. [239, 2026]; [249, 2026].

38.3.2.2 Irregular Warfare and Special Operations working model: inputs, constraints, transforms, outputs, and oversight Evidence anchor. Section 38; [239, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**, with provenance and reviewability throughout.

38.3.2.3 Irregular Warfare and Special Operations knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [239, 2026]; [249, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

38.3.2.4 Irregular Warfare and Special Operations transfer contracts: authority, evidence, tools, and auditable output Evidence anchor. Section 38; [239, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**.
- **Evidence contract:** keep the **Counterintelligence and Source-Integrity Defense** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

38.3.2.5 Irregular Warfare and Special Operations profile emphasis and local focus: method stack and topic cluster Evidence anchor. Section 38; [239, 2026].

The matched profile emphasizes defending institutions, sources, and judgments against deception, insider risk, foreign-intelligence targeting, and source contamination. The method stack is threat awareness, source-descriptor audit, corroboration, anomaly review, red-team challenge, and protected disclosure paths; the local topic cluster is **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**.

38.3.3 Irregular Warfare and Special Operations evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 38; [239, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Counterintelligence and Source-Integrity Defense** profile tells reviewers what evidence is strong enough for the module artifact built around **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**.

38.3.3.1 Irregular Warfare and Special Operations guide source spine: inherited keys and local citation roles Primary guide citations: [239, 2026]; [249, 2026]; [266, 2026]; [276, 2026]; [277, 2026]; [284, 2026]; [288, 2026]; [289, 2026]; [293, 2026]; [112, 2026]; [113, 2026]; [114, 2026]; [115, 2026]; [116, 2026]; [117, 2026]; [118, 2026]; [119, 2026]; [120, 2026]; [308, 2026]; [311, 2026].

38.3.3.2 Irregular Warfare and Special Operations verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [239, 2026]; [249, 2026].

Tier	What counts	How it is used
Source guide	[239, 2026]; [249, 2026]; [266, 2026]; [276, 2026]; [277, 2026]; [284, 2026]; [288, 2026]; [289, 2026]; [293, 2026]; [112, 2026]; [113, 2026]; [114, 2026]; [115, 2026]; [116, 2026]; [117, 2026]; [118, 2026]; [119, 2026]; [120, 2026]; [308, 2026]; [311, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 26's source-canon section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds** and [239, 2026]; [249, 2026], but only directly verified source URLs are encoded as citations.

38.3.3.3 Irregular Warfare and Special Operations intelligence practice lens: evidence artifact and safety check Practice lens: **Dissemination-and-Marking Control Lens** for **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**. [239, 2026]; [249, 2026].

Planning question: Which audience, release authority, marking vocabulary, records duty, and feedback loop governs this intelligence artifact?

Evidence artifact: dissemination map with audience, caveat, marking, records, and feedback fields.

Validation rule: verify source authority, public/classification status, CAPCO-safe vocabulary, audience need, and records disposition before reuse. Applied to **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**.

Handoff contract: deliver release-neutral summaries, source metadata, marking rationale, and review ownership as separate fields.

Safety check: exclude classified content, live release decisions, source-method exposure, and improvised control markings.

38.3.3.4 Irregular Warfare and Special Operations runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 38; [239, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	26.99	26.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Irregular Warfare and Special Operations to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Bounded autonomy, procurement, incident-response, and assurance studio	26.101	26.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Irregular Warfare and Special Operations	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Model-card, recoverability, retention, and learner-support evidence package	26.102	26.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Irregular Warfare and Special Operations	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Hybrid-threat indicator review using sample scenarios and policy thresholds	26.1	26.1 source title transformed into safe curriculum treatment; original: SF Unconventional Warfare Doctrine: TC 18-01	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Hybrid-threat indicator review using sample scenarios and policy thresholds	26.2	26.2 source title transformed into safe curriculum treatment; original: FM 3-05.130: ARSOF Unconventional Warfare	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Hybrid-threat indicator review using sample scenarios and policy thresholds	26.3	26.3 source title transformed into safe curriculum treatment; original: FM 3-05.102: ARSOF Intelligence	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Declassified training-manual archive	26.4	26.4 source title transformed into safe curriculum treatment; original: OSS Origins and Training Manuals (1944)	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Hybrid-threat indicator review using sample scenarios and policy thresholds	26.5	26.5 source title transformed into safe curriculum treatment; original: Principles of Tradecraft for Resistance Organizations	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Hybrid-threat indicator review using sample scenarios and policy thresholds	26.6	26.6 source title transformed into safe curriculum treatment; original: Underground Intelligence Networks: Structure, Security, Continuity	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Hybrid-threat indicator review using sample scenarios and policy thresholds	26.7	26.7 source title transformed into safe curriculum treatment; original: OSS Simple Sabotage Field Manual (1944)	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Hybrid-threat indicator review using sample scenarios and policy thresholds	26.8	26.8 source title transformed into safe curriculum treatment; original: Morale Operations: OSS Psychological Warfare	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings

38.3.3.5 Irregular Warfare and Special Operations reusable subsection contract: topic rows, artifacts, and safety duties Evidence anchor. Section 38; [239, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Hybrid-threat indicator review using sample scenarios and policy thresholds	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
FM 3-05 102: Hybrid-threat indicator review using sample scenarios and policy thresholds	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Declassified training-manual archive	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Principles of Tradecraft for Resistance: Hybrid-threat indicator review using sample scenarios and policy thresholds	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Underground Intelligence Networks: Hybrid-threat indicator review using sample scenarios and policy thresholds	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings

Lesson topic	Practice lens	Evidence artifact	Safety check
OSS Simple Sabotage Field Manual: Hybrid-threat indicator review using sample scenarios and policy thresholds	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Morale Operations: Hybrid-threat indicator review using sample scenarios and policy thresholds	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings

38.3.3.6 Irregular Warfare and Special Operations annotated source ledger: real titles and local contribution Each source cited by this **Counterintelligence and Source-Integrity Defense** module is paired below with its real title and a one-line note on what it contributes to **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**.

Source	Cited work	What it contributes	Status
[239, 2026]	Digital Space and Human Rights	Official OHCHR digital rights portal.	original source-guide
[249, 2026]	GovTech: Putting People First	The official page for the World Bank's Global Program on GovTech and Public Sector Innovation, which helps governments use technology and data to improve public services and governance. It describes support for digital transformation in public administration across areas such as tax administration, public financial management, human resource systems, and citizen engagement, with cross-cutting themes including responsible AI and green digital transformation.	verified source-guide
[266, 2026]	PROV Overview	A W3C Working Group Note from 2013 that provides an overview and roadmap for the PROV family of specifications for representing and exchanging provenance information on the web. It defines provenance as information about the entities, activities, and people involved in producing data, used to assess quality, reliability, and trustworthiness.	verified source-guide
[276, 2026]	What is a Data Protection Impact Assessment and When Is This Mandatory?	A European Data Protection Board FAQ page, part of its data protection guide for small businesses, explaining Data Protection Impact Assessments (DPIAs) and when they are mandatory. It describes a DPIA as a written assessment of the impact of a planned processing operation, required when processing poses high risks to individuals' rights.	verified source-guide
[277, 2026]	Endorsed WP29 Guidelines	This is a European Data Protection Board webpage listing guidelines and documents originating from the Article 29 Working Party that the EDPB endorsed at its first plenary meeting. The catalogued materials relate to the GDPR and cover topics such as consent and transparency, data breach notification, automated decision-making and profiling, data protection impact assessments, data protection officers, and binding corporate rules.	verified source-guide

Source	Cited work	What it contributes	Status
[284, 2026]	Verifiable Credential Data Integrity 1.0	The W3C Recommendation for Verifiable Credential Data Integrity 1.0, published May 2025, defining mechanisms for ensuring the authenticity and integrity of verifiable credentials using cryptographic proofs. It specifies a process of data transformation, hashing, and proof generation, and a corresponding verification procedure, along with a proof data model containing properties such as type, verification method, purpose, and proof value.	verified source-guide
[288, 2026]	Algorithmic Transparency Recording Standard Hub	A GOV.UK collection page serving as the hub for the UK Algorithmic Transparency Recording Standard (ATRS), maintained by the Government Digital Service. It provides a standardized template for documenting public-sector use of algorithmic tools, completion guidance, policy on scope and compliance, and a searchable repository of published transparency records.	verified source-guide
[289, 2026]	Guidance for Organisations Using the Algorithmic Transparency Recording Standard	This is a GOV.UK guidance page published by the Government Digital Service that instructs public sector organizations on completing the Algorithmic Transparency Recording Standard (ATRS) template and publishing their records to the GOV.UK repository. It applies both to central government bodies required to publish under mandatory policy and to other public sector bodies doing so voluntarily.	verified source-guide
[293, 2026]	Inventory of NARA Artificial Intelligence (AI) Use Cases	The National Archives and Records Administration (NARA) official inventory of its artificial intelligence use cases, documenting 14 projects across deployed, pilot, and planned stages. Deployed efforts include workplace productivity tools, automated tagging for museum experiences, and historical record retrieval, while pilots cover PII detection and redaction, semantic search, and metadata generation, and planned work targets FOIA processing and public search.	verified source-guide
[112, 2026]	Full text of “Special Forces Unconventional Warfare”	This U.S. Army Training Circular (TC 18-01) defines the Special Forces concept for planning and conducting unconventional warfare operations, covering how units enable and support resistance movements in denied or hostile territory. It presents a seven-phase operational framework encompassing psychological preparation, infiltration, organization of underground and guerrilla forces, employment, and transition.	verified source-guide

Source	Cited work	What it contributes	Status
[113, 2026]	FM 3-05.130 Army Special Operations Forces Unconventional	U.S. Army Field Manual FM 3-05.130, "Army Special Operations Forces Unconventional Warfare," published by Headquarters, Department of the Army in September 2008. The manual is organized into chapters covering an introduction to warfare types, the instruments of United States national power, national policy and doctrine, and planning considerations including the seven phases of unconventional warfare and the role of Army Special Operations Forces.	verified source-guide
[114, 2026]	Army Special Operations Forces Unconventional Warfare	FM 3-05.130, Army Special Operations Forces Unconventional Warfare (Headquarters, Department of the Army, 30 September 2008). The manual defines unconventional warfare and situates it within U.S. national power, covering the seven phases of UW operations, Special Forces missions, psychological operations, civil affairs operations in the UW context, and the roles of supporting elements including interagency partners. Distribution was restricted to U.S.	verified source-guide
[115, 2026]	Army Special Operations Forces Intelligence	FM 3-05.102, Army Special Operations Forces Intelligence (Headquarters, Department of the Army). The manual addresses intelligence and electronic warfare (IEW) support across Army Special Operations Force components, covering Special Forces, Rangers, ARSOA, PSYOP, and Civil Affairs operations.	verified source-guide
[116, 2026]	Army Special Operations Forces Intelligence	A U.S. Army field manual, FM 3-05.102 (Army Special Operations Forces Intelligence), dated 2001 and superseding FM 34-36, distributed with restrictions to U.S. government agencies. The manual gives special operations forces commanders and staff a doctrinal overview of intelligence support to their missions, covering force structure, training, and operational requirements consistent with joint doctrine.	verified source-guide
[117, 2026]	Office of Strategic Services (OSS) Manuals	An article from Small Wars Journal (affiliated with Arizona State University) announcing that The Resistance Hub has compiled declassified Office of Strategic Services (OSS) manuals for public access. The OSS was the WWII predecessor to the CIA, and the documents illustrate how the United States organized clandestine activities in occupied Europe and Asia.	verified source-guide
[118, 2026]	Special Operations Field Manual, Strategic Services (provisional	A digitized World War II field manual from the Internet Archive, the Special Operations Field Manual, Strategic Services (provisional), issued July 18, 1944 by the U.S. Office of Strategic Services (OSS). The 32-page manual sets out the authorized functions, operational plans, methods, and organization of OSS Maritime Units and the broader Special Operations Branch.	verified source-guide
[119, 2026]	office of strategic services - ARSOF History	See bibliography for scope.	original source-guide

Source	Cited work	What it contributes	Status
[120, 2026]	PRINCIPLES TRADECRAFT	Principles of Tradecraft, a 1995 publication by Militia Free Press (a subsidiary of The Resister). The document presents an overview of intelligence and espionage concepts, with chapters covering an introduction to espionage, agents (typology, identification, recruitment, and handling), and agent organization and management including personnel and structures. It is framed as an introductory treatment rather than a comprehensive reference on intelligence requirements.	verified source-guide
[308, 2026]	Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure	An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure.	verified source-guide
[311, 2026]	Countering Information Threats	An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering.	verified source-guide

Where this sits. This module's overview is Section 38; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

38.3.4 Irregular Warfare and Special Operations governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 38; [239, 2026].

38.3.5 Irregular Warfare and Special Operations analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 26's governance-boundary section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **Counterintelligence and Source-Integrity Defense** for **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**. [239, 2026]; [249, 2026].

Curriculum topic spine: Hybrid-threat indicator review using sample scenarios and policy thresholds, **FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**, **FM 3-05 102: Hybrid-threat indicator review using sample scenarios and policy thresholds**. **Verified anchor cluster:** [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]; [Agency, 2009]; [Jr., 2007]; [Burkett, 2013].

Conceptual depth: defending institutions, sources, and judgments against deception, insider risk, foreign-intelligence targeting, and source contamination.

Method stack: threat awareness, source-descriptor audit, corroboration, anomaly review, red-team challenge, and protected disclosure paths.

Composability contract: identity, access, reporting, corroboration, caveats, and confidence are modeled independently so defensive review can happen without exposure.

Known failure modes: source compromise, deception acceptance, identity overconfidence, insider blind spots, and collapsing CI concerns into undifferentiated IT-security triage.

Defensive boundary: CI content supports defensive awareness, source protection, and analytic integrity; it does not provide surveillance or handling playbooks. Applied to **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**.

Anchor	Why it matters here
[Counterintelligence and Center, 2024]	Official strategy for defensive CI integration, foreign-intelligence threat awareness, strategic advantage protection, and future readiness. Checked as of 2026-05-21; role: curriculum_anchor.
[Archives and Administration, 1981]	Official legal anchor for intelligence authorities, rights-aware collection, analytic competition, oversight, and source-method protection. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026d]	Official sourcing directive for traceability, citations, source descriptors, and source summaries. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2015]	Official ODNI analytic tradecraft standards directive. Checked as of 2026-05-21; role: source_quality_anchor.
[Agency, 2009]	Official structured analytic techniques primer for bias checks, alternatives, and warning analysis. Checked as of 2026-05-21; role: curriculum_anchor.
[Jr., 2007]	Foundational analytic cognition source for bias, mental models, and structured reasoning. Checked as of 2026-06-06; role: curriculum_anchor.
[Burkett, 2013]	A CIA Studies in Intelligence analyst essay arguing that the traditional MICE recruitment-motivation model (Money, Ideology, Compromise, Ego) is better understood through Cialdini's influence principles reframed as RASCLS (Reciprocation, Authority, Scarcity, Commitment/Consistency, Liking, Social Proof), grounding the historical and conceptual lineage of HUMINT recruitment frameworks. Checked as of 2026-06-08; role: curriculum_anchor.

38.3.5.1 Irregular Warfare and Special Operations evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **Counterintelligence and Source-Integrity Defense** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [239, 2026]; [249, 2026].

38.3.6 Irregular Warfare and Special Operations agentic boundary: assist, approve, block, and record

Evidence anchor. Section 38; [239, 2026].

AGEINT translation is bounded by the **Counterintelligence and Source-Integrity Defense** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**.

38.3.6.1 Irregular Warfare and Special Operations permitted defensive utility: curriculum uses and safe outputs **Evidence anchor.**

Section 38; [239, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**.

38.3.6.2 Irregular Warfare and Special Operations excluded operational boundary: blocked actions and stop rules

Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [239, 2026]; [249, 2026] and **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

38.3.7 Irregular Warfare and Special Operations governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 38; [239, 2026].
Governance is practiced as a gate on the **Counterintelligence and Source-Integrity Defense** lane. Learners use the **Dissemination-and-Marking Control Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**.

38.3.7.1 Irregular Warfare and Special Operations governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [239, 2026]; [249, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Counterintelligence and Source-Integrity Defense** failure modes and the **Dissemination-and-Marking Control Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

38.3.7.2 Irregular Warfare and Special Operations evidence package handoff: appendices, records, and reuse **Evidence anchor.** Section 38; [239, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Dissemination-and-Marking Control Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**.

38.3.7.3 Irregular Warfare and Special Operations current-source assurance: verified anchors and local artifact fit The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**. [239, 2026]; [249, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_ncsc_counterintelligence_strategy` for **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**?	The National Counterintelligence Strategy; lane `counterintelligence_source_integrity`; checked 2026-05-21.	dissemination map with audience, caveat, marking, records, and feedback fields; Official strategy for defensive CI integration, foreign-intelligence threat awareness, strategic advantage protection, and future readiness.
What does the module inherit from `official_odni_eo_12333` for **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**?	Executive Order 12333: United States Intelligence Activities; lane `legal_oversight`; checked 2026-05-21.	dissemination map with audience, caveat, marking, records, and feedback fields; Official legal anchor for intelligence authorities, rights-aware collection, analytic competition, oversight, and source-method protection.
What does the module inherit from `official_odni_icd_206` for **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**?	Intelligence Community Directive 206: Sourcing Requirements for Disseminated Analytic Products; lane `analytic_tradecraft`; checked 2026-05-21.	dissemination map with audience, caveat, marking, records, and feedback fields; Official sourcing directive for traceability, citations, source descriptors, and source summaries.
What does the module inherit from `official_odni_icd_203` for **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**?	Intelligence Community Directive 203: Analytic Standards; lane `source_quality_spine`; checked 2026-05-21.	dissemination map with audience, caveat, marking, records, and feedback fields; Official ODNI analytic tradecraft standards directive.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 38; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

38.3.8 Irregular Warfare and Special Operations assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 38; [239, 2026].

38.3.9 Irregular Warfare and Special Operations assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 38; [239, 2026].

38.3.9.1 Irregular Warfare and Special Operations capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**.
Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds** and [239, 2026]; [249, 2026].

38.3.9.2 Irregular Warfare and Special Operations instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds** and [239, 2026]; [249, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

38.3.9.3 Irregular Warfare and Special Operations assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Hybrid-threat indicator review using sample scenarios and policy thresholds	Completed **dissemination map with audience, caveat, marking, records, and feedback fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds	Completed **dissemination map with audience, caveat, marking, records, and feedback fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
FM 3-05 102: Hybrid-threat indicator review using sample scenarios and policy thresholds	Completed **dissemination map with audience, caveat, marking, records, and feedback fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

38.3.10 Irregular Warfare and Special Operations refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [239, 2026]; [249, 2026] and **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**.

38.3.10.1 Irregular Warfare and Special Operations refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**. The local signals begin with [239, 2026]; [249, 2026].

38.3.10.2 Irregular Warfare and Special Operations claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**, and the source spine for these checks begins with [239, 2026]; [249, 2026].

38.3.11 Irregular Warfare and Special Operations reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [239, 2026]; [249, 2026].
Triangulation anchors. In module 26's review-checklist section, directly verified anchors for the **Counterintelligence and Source-Integrity Defense** lane include [Counterintelligence and Center, 2024]; [Archives and Administration, 1981]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2015]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds**. [239, 2026]; [249, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.

- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

38.3.12 Irregular Warfare and Special Operations learning-path links: module map, overview, and curriculum atlas

These links keep **Hybrid-threat indicator review using sample scenarios and policy thresholds; FM 3-05 130: Hybrid-threat indicator review using sample scenarios and policy thresholds** paired with the orientation atlas, the parent unit, and the previous and next modules, so a reader can trace which claims and caveats are inherited rather than re-derived here. Anchored at [239, 2026]; [249, 2026].
Section 2, Section 35, Section 37, Section 39

39 HISTORICAL INTELLIGENCE SERVICES

39.1 HISTORICAL INTELLIGENCE SERVICES learning spine and source route: unit purpose, module order, and evidence handoff

Evidence anchor. Section 39; [266, 2026].

39.1.1 declassified-source interpretation discipline spine: domain question and learning focus

Evidence anchor. Section 39; [266, 2026].
This unit teaches **declassified-source interpretation**. Historical intelligence lessons use archives, redaction caveats, institutional context, and reform lessons without reconstructing live tradecraft.

39.1.2 declassified-source interpretation source-use contract: citation roles and evidence limits

Evidence anchor. Section 39; [266, 2026].
Use source-guide citations and official historical-source anchors for release context, provenance, and oversight lessons.

39.1.3 declassified-source interpretation practice artifact: recurring packet and retained evidence

Evidence anchor. Section 39; [266, 2026].
The recurring practice artifact is a **declassified case-to-principle card** that draws on release metadata, redaction caveat, timeline note, and institutional lesson. The unit keeps its learning spine explicit. Learners mark what the record can support, what redaction leaves unknown, and what institutional lesson survives context shift.

39.1.4 declassified-source interpretation safety boundary: accountable, synthetic, and evidence-bounded limits

No current sources-and-methods reconstruction, operational emulation, or tactical transfer.
This unit introduces the part's governing question, evidence artifacts, source-support spine, and capstone thread before the individual modules begin. [266, 2026]; [267, 2026].
Learners carry one unit capstone thread through the part: define an accountable intelligence question, bind it to source-quality constraints, produce a reviewable artifact, test the artifact against failure modes, and hand it off with enough context for another analyst or instructor to audit. The capstone remains public, synthetic, or owned-lab throughout; its first source anchors are [266, 2026]; [267, 2026].
This unit's deliverables are a source-canon card, claim/evidence ledger, safe-practice lab packet, failure-mode note, instructor rubric, and debrief memo. The full source-lane and evidence-package ledgers appear in the orientation and appendices; this unit introduction keeps only the learner-facing spine for [266, 2026]; [267, 2026].
This unit's safety gates are scope authorization, rights review, data provenance, tool allowlisting, human oversight, rollback, and evidence-bounded output. A missing gate turns the activity into a tabletop, audit, or written governance exercise until the gate is restored against [266, 2026]; [267, 2026].
Capstone thread:

Phase	Artifact	Review gate
Question	accountable learning question and excluded-action list	instructor confirms scope, allowed data, and rights impact
Source canon	source-lane map with guide citations, verified anchors, and refresh dates	citation keys resolve and source identity lock remains stable
Evidence ledger	claim, evidence, uncertainty, confidence, and reviewer register	every material claim has a source, caveat, and owner
Safe lab	synthetic or public dataset packet, tool allowlist, and stop conditions	no live target, private data, external action, or unsafe cyber-physical step
Assurance	evaluation rubric, failure-mode drill, rights map, and remediation note	human reviewer signs off before presentation or reuse
Debrief	capstone memo with lessons, residual risk, refresh triggers, and handoff owner	all unresolved questions and future approvals are explicit

Research lane: Historical and Declassified Intelligence Services. Core anchors: [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]. Conceptual focus: turning declassified records and official histories into safe institutional lessons about analytic judgment, secrecy, oversight, technical-intelligence evolution, and reform. Composability contract: archive source, release channel, historical context, analytic lesson, oversight implication, and modern analogy remain explicitly separated. **Practice lens:** Historical Case-Translation Lens; Which declassified source, release context, institutional lesson, and modern boundary can be carried forward without recreating operations? [266, 2026]; [267, 2026].

39.1.5 HISTORICAL INTELLIGENCE SERVICES visual navigation and module map: evidence flow, order, and safety cues

The unit uses Figure 79 and Figure 80 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 38, Section 40.

39.1.6 HISTORICAL INTELLIGENCE SERVICES module roster and source-lane inventory: citations, lanes, and learner route

Module	Section reference	Source spine
Soviet and Russian Intelligence	Section 40	[266, 2026]; [267, 2026]; [269, 2026]; [278, 2026]; [279, 2026]; [283, 2026]; [290, 2026]; [291, 2026]; [294, 2026]; [121, 2026]; [122, 2026]; [032, 2026]; [021, 2026]; [123, 2026]; [124, 2026]; [125, 2026]; [126, 2026]; [127, 2026]; [022, 2026]; [297, 2026]; [298, 2026].

Module	Section reference	Source spine
American Intelligence History	Section 41	[266, 2026]; [269, 2026]; [271, 2026]; [280, 2026]; [281, 2026]; [282, 2026]; [292, 2026]; [295, 2026]; [296, 2026]; [128, 2026]; [129, 2026]; [117, 2026]; [119, 2026]; [118, 2026]; [130, 2026]; [120, 2026]; [088, 2026]; [089, 2026]; [090, 2026]; [091, 2026]; [131, 2026]; [132, 2026]; [133, 2026]; [019, 2026]; [034, 2026]; [047, 2026]; [038, 2026]; [039, 2026]; [036, 2026]; [297, 2026]; [298, 2026].
British and Allied Intelligence	Section 42	[266, 2026]; [269, 2026]; [270, 2026]; [273, 2026]; [276, 2026]; [285, 2026]; [286, 2026]; [290, 2026]; [294, 2026]; [007, 2026]; [134, 2026]; [011, 2026]; [135, 2026]; [010, 2026]; [041, 2026]; [042, 2026].
Israeli and Continental Services	Section 43	[266, 2026]; [267, 2026]; [271, 2026]; [274, 2026]; [278, 2026]; [280, 2026]; [287, 2026]; [288, 2026]; [295, 2026]; [008, 2026]; [136, 2026]; [297, 2026]; [298, 2026].

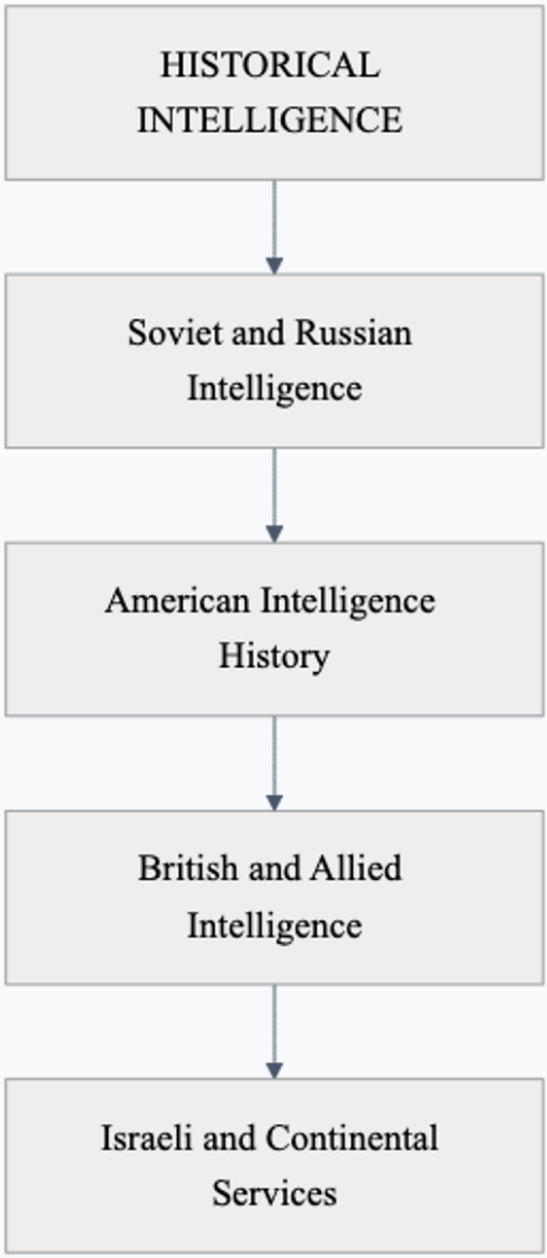


Figure 79: The unit module map traces the part's chapters as a linear reading sequence. In the historical intelligence services section, it lets readers compare 4 module nodes in the unit's ordered, source-backed reading sequence from its first module to its last so the visual functions as a traceable course aid rather than an unscoped assertion.

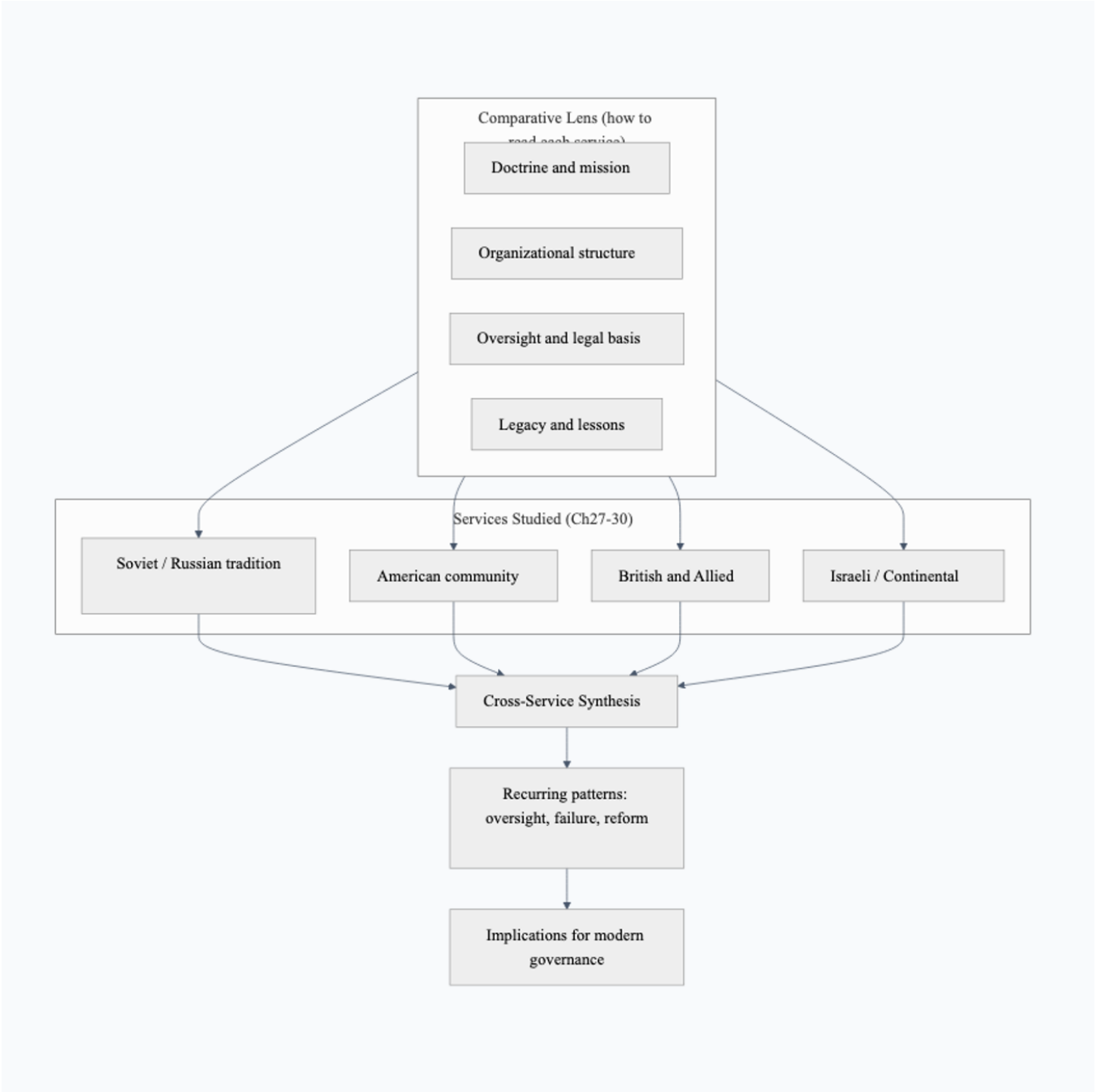


Figure 80: This part applies one comparative lens to four intelligence traditions and folds them into a synthesis that surfaces the recurring patterns of oversight, failure, and reform that shape modern governance. Its reader value is to make Comparative Lens (how to read each service), Doctrine and mission, Organizational structure, and Oversight and legal basis visible at a glance, with the historical intelligence services section as the source section and defensive review as the boundary.

40 Soviet and Russian Intelligence

40.0.1 Soviet and Russian Intelligence figures and course links: visual evidence, source flow, and navigation

The module uses Figure 81 and Figure 79 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 39, Section 41.
This module teaches the **Historical and Declassified Intelligence Services** lane through a bounded, source-backed coursebook chapter. [266, 2026]; [267, 2026].

40.1 Historical and Declassified Intelligence Services frame for Soviet and Russian Intelligence: source context, topic focus, and reader task

Evidence anchor. Section 40; [266, 2026].

40.1.1 Soviet and Russian Intelligence orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 40; [266, 2026].

40.1.2 Soviet and Russian Intelligence conceptual primer: source context, core model, and reader task

This chapter teaches historical intelligence study as declassified evidence review: archives teach institutional lessons when provenance, redaction, context, and modern boundaries are explicit. The chapter uses **Historical Case-Translation Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Declassified source-protection and institutional-control case study; Declassified training-manual archive**.
The central distinction is to separate historical lesson from reconstruction of live tactics or current sources and methods. Core topics include **Declassified source-protection and institutional-control case study; Declassified training-manual archive; Declassified source-protection and agent-handling ethics**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [266, 2026]; [267, 2026].
Learners move from vocabulary and the **Historical Case-Translation Lens** distinction through topic lessons on **Declassified source-protection and institutional-control case study** with evidence and misconception checks, then assemble a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** with safety and rights gates.

40.1.3 Soviet and Russian Intelligence learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 40; [266, 2026].

- Connect **Declassified source-protection and institutional-control case study and Declassified training-manual archive** to **Historical and Declassified Intelligence Services** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate historical lesson from reconstruction of live tactics or current sources and methods; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as romanticized tradecraft, presentist interpretation, redaction overclaiming, decontextualized case reuse, and translating history into operational instructions, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: historical modules use declassified or public records for analysis and governance lessons only; they do not reconstruct live tactics, sources, methods, or current field procedures.

40.1.4 Soviet and Russian Intelligence core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 40; [266, 2026].

Term	Working definition
Declassification context	the release channel, date, and limits of an official historical source
Redaction caveat	the warning that missing text may change interpretation
Institutional lesson	the durable governance or analytic principle drawn from a case
Presentism	the error of forcing modern assumptions onto a historical record
Modern analogy	a bounded comparison that preserves differences between eras
Oversight failure	a documented breakdown in review, records, or accountability visible in the archive
Source-protection lesson	the historical principle about protecting people and methods without reconstructing live tradecraft
Declassified source-protection and…	Key terms: Declassified, protection, institutional.
Declassified training-manual archive	Key terms: Declassified, training, manual.

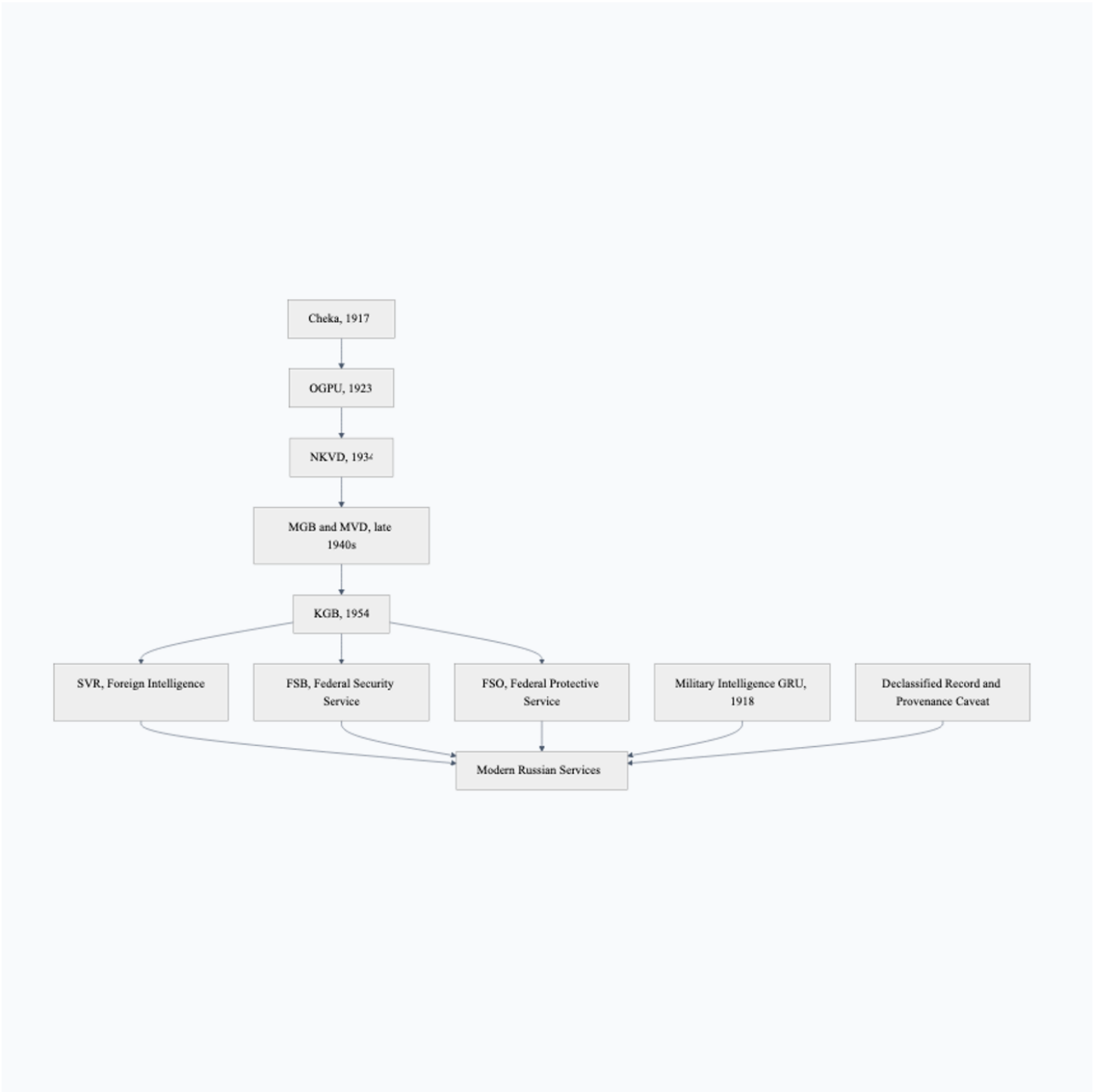


Figure 81: A historical organizational chart tracing the institutional lineage of Soviet and Russian state security from the Cheka to its modern successor services, studied from the declassified record. In the historical intelligence services / soviet and russian intelligence section, it lets readers compare Cheka, 1917, OGPU, 1923, NKVD, 1934, and MGB and MVD, late 1940s so the visual functions as a traceable course aid rather than an unscoped assertion.

40.2 Historical Case-Translation Lens path for Soviet and Russian Intelligence: lesson cluster, safe artifact, and review

Evidence anchor. Section 40; [266, 2026].

40.2.1 Soviet and Russian Intelligence practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 40; [266, 2026].

40.2.2 Soviet and Russian Intelligence topic lessons: source-backed concepts and transfer tasks

This module builds historical intelligence study as declassified evidence review: archives teach institutional lessons when provenance, redaction, context, and modern boundaries are explicit. The sequence opens with **Declassified source-protection and institutional-control case study**, **Declassified training-manual archive**, **Declassified source-protection and agent-handling ethics** and applies the **Historical Case-Translation Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 79; module overview Section 40; curriculum atlas Section 2.

Triangulation anchors. In module 27's topic-lessons section, directly verified anchors for the **Historical and Declassified Intelligence Services** lane include [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]; [Archives and Administration, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

40.2.2.1 Lesson 1: Declassified source-protection and institutional-control case study

Concept. Declassified source-protection and institutional-control case study studies the declassified record for institutional lessons about oversight, source protection, and limits on translating history into practice.

Why it matters. Analysts use **Declassified source-protection** to separate historical lesson from reconstruction of live tactics or current sources and methods. A defensible treatment names the judgment it enables for declassified-source interpretation and case-to-principle translation review, the proof limit that romanticized tradecraft would otherwise hide, and the reviewer accountable for challenge.

Source support. Declassified source-protection and institutional-control case study rests on [121, 2026]. The lead source's own note reads: This is a Blockint blog post by Ludo Block, published in October 2022, analyzing a KGB training manual on information handling released by the Free Russia Foundation. Use it for the working definition that **Declassified source-protection and institutional-control case study** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. For **Declassified source-protection**, reason from the sources cited in this row. [121, 2026] This is a Blockint blog post by Ludo Block, published in October 2022, analyzing a KGB training manual on information handling released by the Free Russia Foundation. The manual, written for foreign intelligence officers, sets out six requirements for valuable intelligence and a framework for evaluating sources based on past performance and competence. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Declassified source-protection**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **Declassified source-protection and institutional-control case**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape **Declassified source-protection** work as a **declassified case-to-principle card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Reuse the **Declassified source-protection** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

40.2.2.2 Lesson 2: Declassified training-manual archive

Concept. Declassified training-manual archive studies the declassified record for institutional lessons about oversight, source protection, and limits on translating history into practice.

Why it matters. Without explicit treatment of **Declassified training-manual archive**, romanticized tradecraft undermines declassified-source interpretation and case-to-principle translation review; the lesson builds the habit to separate historical lesson from reconstruction of live tactics or current sources and methods.

Source support. Declassified training-manual archive rests on [122, 2026]. Use it for the working definition that **Declassified training-manual archive** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. Read **Declassified training-manual archive** against the works cited for this row. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. Build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **Declassified training-manual archive**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape this subject work as a **declassified case-to-principle card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Declassified training-manual archive**: that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Reuse the **Declassified training-manual archive** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

40.2.2.3 Lesson 3: Declassified source-protection and agent-handling ethics

Concept. Declassified source-protection and agent-handling ethics treats agents as software actors with explicit permissions, logs, stop conditions, and human approval—not autonomous decision makers.

Why it matters. Analysts use **Declassified source-protection** to separate historical lesson from reconstruction of live tactics or current sources and methods. A defensible treatment names the judgment it enables for declassified-source interpretation and case-to-principle translation review, the proof limit that romanticized tradecraft would otherwise hide, and the reviewer accountable for challenge.

Source support. Declassified source-protection and agent-handling ethics rests on [032, 2026]. The most specific cited work observes: The 144-page volume is presented as a historical document on Soviet human-intelligence doctrine and counterintelligence practice. Use it for fixing what **Declassified source-protection and agent-handling ethics** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. Read **Declassified source-protection** against the works cited for this row. [032, 2026] A Google Books catalog entry for a 2025 English-translation edition of a Cold War-era Soviet intelligence training manual, published by Century Print Media Group with a translator's note by a retired NATO intelligence officer. The 144-page volume is presented as a historical document on Soviet human-intelligence doctrine and

counterintelligence practice. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. Build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **Declassified source-protection**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape this subject work as a **declassified case-to-principle card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Declassified source-protection**: that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Apply this module's safe boundary for **Declassified source-protection** to another artifact while keeping declassified-source interpretation and case-to-principle translation and reviewer ownership explicit.

40.2.2.4 Lesson 4: Working with Information in Intelligence (1970s)

Concept. Working with Information in Intelligence (1970s) applies Working, Information, in within Historical and Declassified Intelligence Services: learners use separate historical lesson from reconstruction of live tactics or current sources and methods and declassified-source interpretation and case-to-principle translation evidence before any judgment moves forward.

Why it matters. Without explicit treatment of **Working with Information in Intelligence (1970s)**, romanticized tradecraft undermines declassified-source interpretation and case-to-principle translation review; the lesson builds the habit to separate historical lesson from reconstruction of live tactics or current sources and methods.

Source support. Working with Information in Intelligence (1970s) rests on [121, 2026]. The closest source to this row notes: The manual, written for foreign intelligence officers, sets out six requirements for valuable intelligence and a framework for evaluating sources based on past performance and competence. Use it for pinning down the scope of **Working with Information in Intelligence (1970s)**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. For **Working with Information in Intelligence (1970s)**, work from the cited evidence behind this row. [121, 2026] This is a Blockint blog post by Ludo Block, published in October 2022, analyzing a KGB training manual on information handling released by the Free Russia Foundation. The manual, written for foreign intelligence officers, sets out six requirements for valuable intelligence and a framework for evaluating sources based on past performance and competence. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Working with Information in Intelligence (1970s)**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must name the source descriptor, the bounded claim about **Working with Information in Intelligence**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape this subject work as a **declassified case-to-principle card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that Working with Information in Intelligence (1970s) is optional whenever separate historical lesson from reconstruction of live tactics or current sources and methods feels inconvenient.

Transfer task. Transfer **Working with Information in Intelligence (1970s)** to a second module by preserving declassified-source interpretation and case-to-principle translation, changing the source evidence, and naming a new reviewer.

40.2.2.5 Lesson 5: Declassified psychological-pressure ethics

Concept. Declassified psychological-pressure ethics studies the declassified record for institutional lessons about source protection, oversight, and the danger of translating historical methods into current practice.

Why it matters. Declassified psychological-pressure ethics matters in the **Historical and Declassified Intelligence Services** lane because declassified-source interpretation and case-to-principle translation evidence must stay separate from judgment; romanticized tradecraft is a common failure.

Source support. Declassified psychological-pressure ethics rests on [021, 2026]. Its anchor reference records: The article describes how the manuals cover intelligence methods such as agent recruitment, psychological manipulation, and disinformation detection, and notes the materials remain relevant because related methods persist in modern Russian services. Use it for the claim that **Declassified psychological-pressure ethics** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. For **Declassified psychological-pressure ethics**, reason from the sources cited in this row. [021, 2026] A July 2019 story from The World (PRX public radio) about a project led by Michael Weiss to translate previously unpublished Soviet-era KGB training manuals from the 1970s-80s into English. The article describes how the manuals cover intelligence methods such as agent recruitment, psychological manipulation, and disinformation detection, and notes the materials remain relevant because related methods persist in modern Russian services. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. Build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **Declassified psychological-pressure ethics**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape this subject work as a **declassified case-to-principle card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Declassified psychological-pressure ethics**: that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Apply this module's safe boundary for **Declassified psychological-pressure ethics** to another artifact while keeping declassified-source interpretation and case-to-principle translation and reviewer ownership explicit.

40.2.2.6 Lesson 6: Some Aspects of Training Agents Psychologically (1985)

Concept. Some Aspects of Training Agents Psychologically (1985) applies Some, Aspects, Training within Historical and Declassified Intelligence Services: learners use separate historical lesson from reconstruction of live tactics or current sources and methods and declassified-source interpretation and case-to-principle translation evidence before any judgment moves forward.

Why it matters. Some Aspects matters in the **Historical and Declassified Intelligence Services** lane because declassified-source interpretation and case-to-principle translation evidence must stay separate from judgment; romanticized tradecraft is a common failure.

Source support. Some Aspects of Training Agents Psychologically (1985) rests on [021, 2026]. The lead source's own note reads: The article describes how the manuals cover intelligence methods such as agent recruitment, psychological manipulation, and disinformation detection, and notes the materials remain relevant because related methods persist in modern Russian services. Use it for fixing what **Some Aspects of Training Agents Psychologically (1985)** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. For **Some Aspects**, reason from the sources cited in this row. [021, 2026] A July 2019 story from The World (PRX public radio) about a project led by Michael Weiss to translate previously unpublished Soviet-era KGB training manuals from the 1970s-80s into English. The article describes how the manuals cover intelligence methods such as agent recruitment, psychological manipulation, and disinformation detection, and notes the materials remain relevant because related methods persist in modern Russian services. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Some Aspects**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must name the source descriptor, the bounded claim about **Some Aspects of Training Agents**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Some Aspects** work as a **declassified case-to-principle card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that Some Aspects of Training Agents Psychologically (1985) replaces human review whenever evidence looks plausible.

Transfer task. Transfer **Some Aspects** to a second module by preserving declassified-source interpretation and case-to-principle translation, changing the source evidence, and naming a new reviewer.

40.2.2.7 Lesson 7: Exposure of Disinformation in Intelligence Materials (1968)

Concept. Exposure of Disinformation in Intelligence Materials (1968) analyzes influence campaigns through provenance, audience harm, attribution caution, and transparent response options.

Why it matters. Analysts use **Exposure of Disinformation in Intelligence Materials (1968)** to separate historical lesson from reconstruction of live tactics or current sources and methods. A defensible treatment names the judgment it enables for declassified-source interpretation and case-to-principle translation review, the proof limit that romanticized tradecraft would otherwise hide, and the reviewer accountable for challenge.

Source support. Exposure of Disinformation in Intelligence Materials (1968) rests on [021, 2026]. The most specific cited work observes: The article describes how the manuals cover intelligence methods such as agent recruitment, psychological manipulation, and disinformation detection, and notes the materials remain relevant because related methods persist in modern Russian services. Use it for fixing what **Exposure of Disinformation in Intelligence Materials (1968)** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. For **Exposure of Disinformation in Intelligence Materials (1968)**, work from the cited evidence behind this row. [021, 2026] A July 2019 story from The World (PRX public radio) about a project led by Michael Weiss to translate previously unpublished Soviet-era KGB training manuals from the 1970s-80s into English. The article describes how the manuals cover intelligence methods such as agent recruitment, psychological manipulation, and disinformation detection, and notes the materials remain relevant because related methods persist in modern Russian services. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Exposure of Disinformation in Intelligence Materials (1968)**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must name the source descriptor, the bounded claim about **Exposure of Disinformation in Intelligence**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape this subject work as a **declassified case-to-principle card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that Exposure of Disinformation in Intelligence Materials (1968) can be used while ignoring the rule to separate historical lesson from reconstruction of live tactics or current sources and methods.

Transfer task. Transfer **Exposure of Disinformation in Intelligence Materials (1968)** to a second module by preserving declassified-source interpretation and case-to-principle translation, changing the source evidence, and naming a new reviewer.

40.2.2.8 Lesson 8: Organizational Structure and Management of Intelligence Residency

Concept. Organizational Structure and Management of Intelligence Residency applies Organizational, Structure, Management within Historical and Declassified Intelligence Services: learners use separate historical lesson from reconstruction of live tactics or current sources and methods and declassified-source interpretation and case-to-principle translation evidence before any judgment moves forward.

Why it matters. Organizational Structure matters in the **Historical and Declassified Intelligence Services** lane because declassified-source interpretation and case-to-principle translation evidence must stay separate from judgment; romanticized tradecraft is a common failure.

Source support. Organizational Structure and Management of Intelligence Residency rests on [297, 2026] and [298, 2026]. The closest source to this row notes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for the working definition that **Organizational Structure and Management of Intelligence Residency** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. Ground **Organizational Structure** in the evidence the row cites. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Organizational Structure**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must name the source descriptor, the bounded claim about **Organizational Structure and Management of**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Organizational Structure** work as a **declassified case-to-principle card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that Organizational Structure and Management of Intelligence Residency is optional whenever separate historical lesson from reconstruction of live tactics or current sources and methods feels inconvenient.

Transfer task. Transfer **Organizational Structure** to a second module by preserving declassified-source interpretation and case-to-principle translation, changing the source evidence, and naming a new reviewer.

40.2.2.9 Lesson 9: Declassified confidential-contact oversight

Concept. Declassified confidential-contact oversight studies the declassified record for institutional lessons about source protection, oversight, and the danger of translating historical methods into current practice.

Why it matters. Declassified confidential-contact oversight connects classroom vocabulary to Historical and Declassified Intelligence Services practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Declassified confidential-contact oversight rests on [122, 2026]. Use it for pinning down the scope of **Declassified confidential-contact oversight**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. Ground **Declassified confidential-contact oversight** in the evidence the row cites. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. Build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **Declassified confidential-contact oversight**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape this subject work as a **declassified case-to-principle card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Declassified confidential-contact oversight**: that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Reuse the **Declassified confidential-contact oversight** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

40.2.2.10 Lesson 10: Declassified residency-management oversight **Concept. Declassified residency-management oversight** studies the declassified record for institutional lessons about oversight, source protection, and limits on translating history into practice.

Why it matters. Declassified residency-management oversight matters in the **Historical and Declassified Intelligence Services** lane because declassified-source interpretation and case-to-principle translation evidence must stay separate from judgment; romanticized tradecraft is a common failure.

Source support. Declassified residency-management oversight rests on [122, 2026]. Use it for fixing what **Declassified residency-management oversight** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. For **Declassified residency-management oversight**, work from the cited evidence behind this row. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. Build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **Declassified residency-management oversight**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape this subject work as a **declassified case-to-principle card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Declassified residency-management oversight**: that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Apply this module's safe boundary for **Declassified residency-management oversight** to another artifact while keeping declassified-source interpretation and case-to-principle translation and reviewer ownership explicit.

40.2.2.11 Lesson 11: Declassified special-unit oversight case **Concept. Declassified special-unit oversight case** studies the declassified record for institutional lessons about oversight, source protection, and limits on translating history into practice.

Why it matters. Analysts use **Declassified special-unit oversight case** to separate historical lesson from reconstruction of live tactics or current sources and methods. A defensible treatment names the judgment it enables for declassified-source interpretation and case-to-principle translation review, the proof limit that romanticized tradecraft would otherwise hide, and the reviewer accountable for challenge.

Source support. Declassified special-unit oversight case rests on [123, 2026]. Its anchor reference records: Dolmatov, accompanied by an extensive preface by Western trainer Jim Shortt. Use it for fixing what **Declassified special-unit oversight case** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. For **Declassified special-unit oversight case**, reason from the sources cited in this row. [123, 2026] A 1993 Paladin Press publication presenting a translated Soviet special-operations training text attributed to A. I. Dolmatov, accompanied by an extensive preface by Western trainer Jim Shortt. The preface traces the evolution of Soviet special forces from the 1917 revolution through the Cold War and describes organizations such as the KGB, MVD, and GRU and units including Alpha, Spetsnaz, and OMON. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. Build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **Declassified special-unit oversight case**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape this subject work as a **declassified case-to-principle card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Declassified special-unit oversight case**: that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Reuse the **Declassified special-unit oversight case** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

40.2.2.12 Lesson 12: Mitrokhin Archive: Declassified source-protection and institutional-control case study **Concept. Mitrokhin Archive: Declassified source-protection and institutional-control case study** studies the declassified record for institutional lessons about oversight, source protection, and limits on translating history into practice.

Why it matters. Without explicit treatment of **Mitrokhin Archive**, romanticized tradecraft undermines declassified-source interpretation and case-to-principle translation review; the lesson builds the habit to separate historical lesson from reconstruction of live tactics or current sources and methods.

Source support. Mitrokhin Archive: Declassified source-protection and institutional-control case study rests on [124, 2026], [125, 2026], and [126, 2026]. The closest source to this row notes: Zinoviev faced professional retaliation including revocation of his doctorate and expulsion from the Communist Party following the publication of satirical anti-Soviet works such as Yawning Heights. Use them for fixing what **Mitrokhin Archive: Declassified source-protection and institutional-control case study** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. For **Mitrokhin Archive**, work from the cited evidence behind this row. [124, 2026] This article draws on the Mitrokhin Archive, compiled by defected KGB archivist Vasili Mitrokhin, to document Soviet state surveillance of dissident philosopher Alexander Zinoviev, who was assigned the codename Logician by the KGB's Fifth Chief Directorate. Zinoviev faced professional retaliation including revocation of his doctorate and expulsion from the Communist Party following the publication of satirical anti-Soviet works such as Yawning Heights. [125, 2026] The Wilson Center Digital Archive link for the Mitrokhin Archive is a dead staging domain. The Mitrokhin Archive documents Soviet KGB history; use the published Cambridge University Press edition or Wilson Center production archive instead. [126, 2026] A Wikipedia article on the Mitrokhin Archive, a collection of handwritten notes made by KGB archivist Vasili Mitrokhin documenting Soviet intelligence operations from the 1930s through the 1980s. Mitrokhin secretly copied files between 1972 and 1984 while overseeing the relocation of KGB foreign intelligence archives, and after the Soviet collapse defected to the UK in 1992 with the material. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Mitrokhin Archive**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **Mitrokhin Archive**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape **Mitrokhin Archive** work as a **declassified case-to-principle card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Transfer **Mitrokhin Archive** from this module to a second motif by preserving declassified-source interpretation and case-to-principle translation, replacing action with audit, and naming the blocked use.

40.2.2.13 Lesson 13: GRU: Soviet Military Intelligence Structure **Concept. GRU: Soviet Military Intelligence Structure** applies GRU, Soviet, Military within Historical and Declassified Intelligence Services: learners use separate historical lesson from reconstruction of live tactics or current sources and methods and declassified-source interpretation and case-to-principle translation evidence before any judgment moves forward.

Why it matters. GRU: Soviet Military Intelligence Structure matters in the **Historical and Declassified Intelligence Services** lane because declassified-source interpretation and case-to-principle translation evidence must stay separate from judgment; romanticized tradecraft is a common failure.

Source support. GRU: Soviet Military Intelligence Structure rests on [297, 2026] and [298, 2026]. The closest source to this row notes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for the working definition that **GRU: Soviet Military Intelligence Structure** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. Read **GRU: Soviet Military Intelligence Structure** against the works cited for this row. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **GRU**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must name the source descriptor, the bounded claim about **GRU**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **GRU: Soviet Military Intelligence Structure** work as a **declassified case-to-principle card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that GRU: Soviet Military Intelligence Structure establishes intent without reviewing alternative explanations.

Transfer task. Transfer **GRU: Soviet Military Intelligence Structure** to a second module by preserving declassified-source interpretation and case-to-principle translation, changing the source evidence, and naming a new reviewer.

40.2.2.14 Lesson 14: Interpreter Magazine: Declassified source-protection and institutional-control case study **Concept. Interpreter Magazine: Declassified source-protection and institutional-control case study** studies the declassified record for institutional lessons about oversight, source protection, and limits on translating history into practice.

Why it matters. Interpreter Magazine connects classroom vocabulary to Historical and Declassified Intelligence Services practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Interpreter Magazine: Declassified source-protection and institutional-control case study rests on [022, 2026]. Its anchor reference records: An article from The Interpreter, a publication focused on Russian affairs and disinformation, announcing a project to translate, analyze, and publish previously unpublished Soviet KGB training documents. Use it for the claim that **Interpreter Magazine: Declassified source-protection and institutional-control case study** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. For **Interpreter Magazine**, reason from the sources cited in this row. [022, 2026] An article from The Interpreter, a publication focused on Russian affairs and disinformation, announcing a project to translate, analyze, and publish previously unpublished Soviet KGB training documents. It summarizes a set of newly obtained manuals spanning several decades and describes the topics they cover, including operational terminology, agent classification, information-gathering methods, recruitment and vetting procedures, and counterintelligence concerns. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Interpreter Magazine**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **Interpreter Magazine**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape **Interpreter Magazine** work as a **declassified case-to-principle card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Transfer **Interpreter Magazine** from this module to a second motif by preserving declassified-source interpretation and case-to-principle translation, replacing action with audit, and naming the blocked use.

40.2.3 Soviet and Russian Intelligence worked safe example: synthetic inputs, evidence, and review

Worked example: a sample seminar studies a declassified reform episode and extracts an oversight lesson without reconstructing current sources and methods. [266, 2026]; [267, 2026].

Triangulation anchors. In module 27's worked-example section, directly verified anchors for the **Historical and Declassified Intelligence Services** lane include [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]; [Archives and Administration, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **declassified-source interpretation**. Learners use a **declassified case-to-principle card** and keep this boundary visible: No current sources-and-methods reconstruction, operational emulation, or tactical transfer.

Frame. The classroom question centers on **Declassified source-protection and institutional-control case study**. Excluded actions stay explicit, and the **Historical Case-Translation Lens** planning question is: Which declassified source, release context, institutional lesson, and modern boundary can be carried forward without recreating operations?

Inputs. For the **Declassified source-protection and institutional-control case study** scenario, use public archive metadata, a short excerpt, a timeline template, and an oversight-question worksheet. The Historical Case-Translation Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Declassified source-protection and institutional-control case study**, students record provenance, mark redactions, build timeline, distinguish known from unknown, and extract a governance lesson. Pause whenever an inference about Declassified source-protection and institutional-control case study appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Declassified source-protection and institutional-control case study** classroom scenario; unit artifact = declassified case-to-principle card; evidence = allowed inputs; method = declassified-source interpretation and case-to-principle translation; output = a historical case card with release context, caveats, lesson, and evidence-bounded boundary; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Declassified source-protection and institutional-control case study** as "Historical Case-Translation Lens confirms it" is not enough. The revision ties the claim to declassified-source interpretation and case-to-principle translation, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Declassified source-protection and institutional-control case study** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

40.2.4 Soviet and Russian Intelligence practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Historical Case-Translation Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Declassified source-protection and institutional-control case study; Declassified training-manual archive**.

Triangulation anchors. In module 27's practice-sequence section, directly verified anchors for the **Historical and Declassified Intelligence Services** lane include [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]; [Archives and Administration, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Declassified source-protection and institutional-control case study, Declassified training-manual archive, Declassified source-protection and agent-handling ethics; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Historical and Declassified Intelligence Services** lane.
2. Frame	Answer the lens question: Which declassified source, release context, institutional lesson, and modern boundary can be carried forward without recreating operations?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Declassified source-protection and institutional-control case study: historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the declassified case-to-principle card fields for Declassified source-protection and institutional-control case study.	Unit profile note.	Evidence artifacts include release metadata, redaction caveat.
4. Challenge	Test the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.	Failure-mode note.	The artifact applies the key distinction: separate historical lesson from reconstruction of live tactics or current sources and methods.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

40.2.4.1 Soviet and Russian Intelligence instructor notes: source reasoning, review points, and studio focus Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Declassified source-protection and institutional-control case study; Declassified training-manual archive**. [266, 2026]; [267, 2026].

40.2.4.2 Soviet and Russian Intelligence extension exercise: peer validation and refresh trigger review **Evidence anchor.** Section 40; [266, 2026].

Have learners swap artifacts and apply the **Historical Case-Translation Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Declassified source-protection and institutional-control case study; Declassified training-manual archive**.

40.2.5 Soviet and Russian Intelligence knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 40; [266, 2026].

1. Explain how **Declassified source-protection and institutional-control case study** is defined here; name the source descriptor that supports the definition.
2. Contrast **Declassified source-protection and institutional-control case study** with **Declassified training-manual archive** using the **Historical Case-Translation Lens** artifact fields.
3. Identify one failure mode from the **Historical and Declassified Intelligence Services** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which institutional lesson is defensible from the record, and which claim reconstructs live tradecraft?
5. Correct this misconception: that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

40.2.5.1 Soviet and Russian Intelligence answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Declassified source-protection and institutional-control case study** without source evidence, uncertainty, or a safe transfer task.

40.3 Soviet and Russian Intelligence assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 40; [266, 2026].

40.3.1 Soviet and Russian Intelligence evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 40; [266, 2026].

40.3.2 Soviet and Russian Intelligence transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 40; [266, 2026].

40.3.2.1 Soviet and Russian Intelligence lineage and source tradition: profile, concepts, and first anchors This sits in the **Historical and Declassified Intelligence Services** lineage: turning declassified records and official histories into safe institutional lessons about analytic judgment, secrecy, oversight, technical-intelligence evolution, and reform. [266, 2026]; [267, 2026].

40.3.2.2 Soviet and Russian Intelligence working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 40; [266, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Declassified source-protection and institutional-control case study; Declassified training-manual archive**, with provenance and reviewability throughout.

40.3.2.3 Soviet and Russian Intelligence knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [266, 2026]; [267, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

40.3.2.4 Soviet and Russian Intelligence transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 40; [266, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Declassified source-protection and institutional-control case study; Declassified training-manual archive**.
- **Evidence contract:** keep the **Historical and Declassified Intelligence Services** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

40.3.2.5 Soviet and Russian Intelligence profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 40; [266, 2026].

The matched profile emphasizes turning declassified records and official histories into safe institutional lessons about analytic judgment, secrecy, oversight, technical-intelligence evolution, and reform. The method stack is provenance review, declassification-status notation, institutional timeline building, case-to-principle translation, and uncertainty about redacted records; the local topic cluster is **Declassified source-protection and institutional-control case study; Declassified training-manual archive**.

40.3.3 Soviet and Russian Intelligence evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 40; [266, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Historical and Declassified Intelligence Services** profile tells reviewers what evidence is strong enough for the module artifact built around **Declassified source-protection and institutional-control case study; Declassified training-manual archive**.

40.3.3.1 Soviet and Russian Intelligence guide source spine: inherited keys and local citation roles Primary guide citations: [266, 2026]; [267, 2026]; [269, 2026]; [278, 2026]; [279, 2026]; [283, 2026]; [290, 2026]; [291, 2026]; [294, 2026]; [121, 2026]; [122, 2026]; [032, 2026]; [021, 2026]; [123, 2026]; [124, 2026]; [125, 2026]; [126, 2026]; [127, 2026]; [022, 2026]; [297, 2026]; [298, 2026].

40.3.3.2 Soviet and Russian Intelligence verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [266, 2026]; [267, 2026].

Tier	What counts	How it is used
Source guide	[266, 2026]; [267, 2026]; [269, 2026]; [278, 2026]; [279, 2026]; [283, 2026]; [290, 2026]; [291, 2026]; [294, 2026]; [121, 2026]; [122, 2026]; [032, 2026]; [021, 2026]; [123, 2026]; [124, 2026]; [125, 2026]; [126, 2026]; [127, 2026]; [022, 2026]; [297, 2026]; [298, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 27's source-canon section, directly verified anchors for the **Historical and Declassified Intelligence Services** lane include [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]; [Archives and Administration, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **Declassified source-protection and institutional-control case study; Declassified training-manual archive** and [266, 2026]; [267, 2026], but only directly verified source URLs are encoded as citations.

40.3.3.3 Soviet and Russian Intelligence intelligence practice lens: evidence artifact and safety check Practice lens: **Historical Case-Translation Lens** for **Declassified source-protection and institutional-control case study; Declassified training-manual archive**. [266, 2026]; [267, 2026].

Planning question: Which declassified source, release context, institutional lesson, and modern boundary can be carried forward without recreating operations?

Evidence artifact: historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary.

Validation rule: distinguish what the record shows, what remains redacted or unknown, and which governance lesson is defensibly transferable. Applied to **Declassified source-protection and institutional-control case study; Declassified training-manual archive**.

Handoff contract: handoff preserves archive citation, historical context, analytic lesson, oversight implication, and modern analogy as separate fields.

Safety check: exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material.

40.3.3.4 Soviet and Russian Intelligence runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 40; [266, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	27.99	27.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Soviet and Russian Intelligence to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Bounded autonomy, procurement, incident-response, and assurance studio	27.101	27.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Soviet and Russian Intelligence	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Model-card, recoverability, retention, and learner-support evidence package	27.102	27.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Soviet and Russian Intelligence	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified source-protection and institutional-control case study	27.1	27.1 source title transformed into safe curriculum treatment; original: KGB Structure, Culture, and Doctrine: First Chief Directorate	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Declassified training-manual archive	27.2	27.2 source title transformed into safe curriculum treatment; original: The Lubyanka Files: 29 KGB Training Manuals, 1965–1989	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified source-protection and agent-handling ethics	27.2.1	27.2.1 source title transformed into safe curriculum treatment; original: Working with Agents (Declassified Manual)	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Working with Information in Intelligence (1970s)	27.2.2	27.2.2 Working with Information in Intelligence (1970s)	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified psychological-pressure ethics	27.2.3	27.2.3 source title transformed into safe curriculum treatment; original: Psychological Methods and Manipulation of Agents (1988)	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Some Aspects of Training Agents Psychologically (1985)	27.2.4	27.2.4 Some Aspects of Training Agents Psychologically (1985)	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Exposure of Disinformation in Intelligence Materials (1968)	27.2.5	27.2.5 Exposure of Disinformation in Intelligence Materials (1968)	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Organizational Structure and Management of Intelligence Residency	27.2.6	27.2.6 Organizational Structure and Management of Intelligence Residency	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified confidential-contact oversight	27.2.7	27.2.7 source title transformed into safe curriculum treatment; original: On Organizing Work with Confidential Contacts	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified residency-management oversight	27.2.8	27.2.8 source title transformed into safe curriculum treatment; original: Tasks of a KGB Resident Abroad	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified special-unit oversight case	27.3	27.3 source title transformed into safe curriculum treatment; original: KGB Alpha Team Training Manual	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified source-protection and institutional-control case study	27.4	27.4 source title transformed into safe curriculum treatment; original: The Mitrokhin Archive: KGB Global Operations	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
GRU: Soviet Military Intelligence Structure	27.5	27.5 GRU: Soviet Military Intelligence Structure	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified source-protection and institutional-control case study	27.6	27.6 source title transformed into safe curriculum treatment; original: The Interpreter Magazine: KGB Manual Summaries	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material

40.3.3.5 Soviet and Russian Intelligence reusable subsection contract: topic rows, artifacts, and safety duties **Evidence anchor.** Section 40; [266, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Declassified source-protection and institutional-control case study	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified training-manual archive	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified source-protection and agent-handling ethics	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Working with Information in Intelligence (1970s)	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified psychological-pressure ethics	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Some Aspects of Training Agents Psychologically (1985)	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Exposure of Disinformation in Intelligence Materials (1968)	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Organizational Structure and Management of Intelligence Residency	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified confidential-contact oversight	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified residency-management oversight	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified special-unit oversight case	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Mitrokhin Archive: Declassified source-protection and institutional-control case study	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
GRU: Soviet Military Intelligence Structure	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Interpreter Magazine: Declassified source-protection and institutional-control case study	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material

40.3.3.6 Soviet and Russian Intelligence annotated source ledger: real titles and local contribution Each source cited by this **Historical and Declassified Intelligence Services** module is paired below with its real title and a one-line note on what it contributes to **Declassified source-protection and institutional-control case study; Declassified training-manual archive**.

Source	Cited work	What it contributes	Status
[266, 2026]	PROV Overview	A W3C Working Group Note from 2013 that provides an overview and roadmap for the PROV family of specifications for representing and exchanging provenance information on the web. It defines provenance as information about the entities, activities, and people involved in producing data, used to assess quality, reliability, and trustworthiness.	verified source-guide
[267, 2026]	PROV-O: The PROV Ontology	The W3C Recommendation for PROV-O, published in April 2013, which expresses the PROV data model as an OWL2 ontology for representing provenance information across systems. It defines three core classes, Entity, Activity, and Agent, and organizes terms into starting-point, expanded, and qualified categories.	verified source-guide
[269, 2026]	Data on the Web Best Practices	A W3C Recommendation, "Data on the Web Best Practices," published January 31, 2017 by the Data on the Web Best Practices Working Group. It offers 35 best practices for publishing and consuming data on the Web, covering metadata, licensing and provenance, data quality, dataset versioning, persistent URIs, machine-readable formats, vocabulary reuse, access methods, preservation, and feedback.	verified source-guide
[278, 2026]	Recommendation of the Council on Public Procurement	The OECD Recommendation of the Council on Public Procurement (OECD/LEGAL/0411), a legal instrument adopted by the OECD Council in 2015 on the proposal of the Public Governance Committee. It frames public procurement as a pillar of strategic governance and service delivery and sets out principles for governments to follow.	verified source-guide
[279, 2026]	Open Contracting Data Standard	The documentation homepage for the Open Contracting Data Standard, version 1.1.5, maintained by the Open Contracting Partnership to support disclosure of government contracting data across the procurement lifecycle. It provides a common data model spanning planning, tender, award, contract, and implementation stages, along with a primer, implementation guidance, technical schemas, and validation tooling.	verified source-guide
[283, 2026]	Recommendation of the Council on Open Government	An OECD legal instrument document reproducing the Recommendation of the Council on Open Government (OECD/LEGAL/0438), adopted on 14 December 2017. It defines open government as a culture of governance promoting transparency, integrity, accountability, and stakeholder participation in support of democracy and inclusive growth.	verified source-guide

Source	Cited work	What it contributes	Status
[290, 2026]	NIST SP 800-218A: Secure Software Development Practices for Generative AI and Dual-Use Foundation Models	NIST Special Publication 800-218A (July 2024), which augments the Secure Software Development Framework with practices specific to AI model development across the software lifecycle. Produced in response to Executive Order 14110, it addresses AI model producers, developers building on those models, and acquirers of AI systems, and is designed to be used alongside NIST SP 800-218.	verified source-guide
[291, 2026]	Revised 508 Standards and 255 Guidelines	Official documentation from the U.S. Access Board on the Revised 508 Standards and 255 Guidelines for information and communication technology accessibility. It establishes mandatory accessibility requirements for federal agencies and voluntary guidelines for telecommunications manufacturers, covering hardware, software, websites, electronic documents, and support services.	verified source-guide
[294, 2026]	M-25-21: Accelerating Federal Use of AI through Innovation, Governance, and Public Trust	An April 2025 Office of Management and Budget memorandum (M-25-21) directing executive branch agencies on federal use of artificial intelligence. Issued under Executive Order 14179, it instructs agencies to accelerate adoption of AI to improve public services and government efficiency while maintaining safeguards for civil rights, civil liberties, and privacy.	verified source-guide
[121, 2026]	How the KGB handled information - Blockint	This is a Blockint blog post by Ludo Block, published in October 2022, analyzing a KGB training manual on information handling released by the Free Russia Foundation. The manual, written for foreign intelligence officers, sets out six requirements for valuable intelligence and a framework for evaluating sources based on past performance and competence.	verified source-guide
[122, 2026]	The Lubyanka Files - Free Russia Foundation THINK TANK	See bibliography for scope.	verified source-guide
[032, 2026]	Cited source (see bibliography)	A Google Books catalog entry for a 2025 English-translation edition of a Cold War-era Soviet intelligence training manual, published by Century Print Media Group with a translator's note by a retired NATO intelligence officer. The 144-page volume is presented as a historical document on Soviet human-intelligence doctrine and counterintelligence practice.	verified source-guide
[021, 2026]	Learn how to be a spy from previously unpublished KGB training	A July 2019 story from The World (PRX public radio) about a project led by Michael Weiss to translate previously unpublished Soviet-era KGB training manuals from the 1970s-80s into English. The article describes how the manuals cover intelligence methods such as agent recruitment, psychological manipulation, and disinformation detection, and notes the materials remain relevant because related methods persist in modern Russian services.	verified source-guide

Source	Cited work	What it contributes	Status
[123, 2026]	Full text of "KGB Alpha Team Training Manual" - Internet Archive	A 1993 Paladin Press publication presenting a translated Soviet special-operations training text attributed to A. I. Dolmatov, accompanied by an extensive preface by Western trainer Jim Shortt. The preface traces the evolution of Soviet special forces from the 1917 revolution through the Cold War and describes organizations such as the KGB, MVD, and GRU and units including Alpha, Spetsnaz, and OMON.	verified source-guide
[124, 2026]	The Logician (The Zinoviev's case). Folder 46. The Chekist	This article draws on the Mitrokhin Archive, compiled by defected KGB archivist Vasili Mitrokhin, to document Soviet state surveillance of dissident philosopher Alexander Zinoviev, who was assigned the codename Logician by the KGB's Fifth Chief Directorate. Zinoviev faced professional retaliation including revocation of his doctorate and expulsion from the Communist Party following the publication of satirical anti-Soviet works such as Yawning Heights.	verified source-guide
[125, 2026]	Mitrokhin Archive	The Wilson Center Digital Archive link for the Mitrokhin Archive is a dead staging domain. The Mitrokhin Archive documents Soviet KGB history; use the published Cambridge University Press edition or Wilson Center production archive instead.	verified source-guide
[126, 2026]	Mitrokhin Archive	A Wikipedia article on the Mitrokhin Archive, a collection of handwritten notes made by KGB archivist Vasili Mitrokhin documenting Soviet intelligence operations from the 1930s through the 1980s. Mitrokhin secretly copied files between 1972 and 1984 while overseeing the relocation of KGB foreign intelligence archives, and after the Soviet collapse defected to the UK in 1992 with the material.	verified source-guide context; do not use as primary analytic support
[127, 2026]	The Mitrokhin archive : the KGB and the world	An Internet Archive record for The Mitrokhin Archive: The KGB and the World, a two-volume work by Christopher Andrew published in 1999 by Allen Lane, running to roughly 1,050 pages. The volumes draw on materials compiled by former KGB officer Vasili Mitrokhin to document Soviet intelligence operations, with the first volume covering the KGB in Europe and the West and the second addressing the KGB and the wider world.	verified source-guide
[022, 2026]	Summaries of Newly Obtained KGB Training Manuals - The Interpreter	An article from The Interpreter, a publication focused on Russian affairs and disinformation, announcing a project to translate, analyze, and publish previously unpublished Soviet KGB training documents. It summarizes a set of newly obtained manuals spanning several decades and describes the topics they cover, including operational terminology, agent classification, information-gathering methods, recruitment and vetting procedures, and counterintelligence concerns.	verified source-guide

Source	Cited work	What it contributes	Status
[297, 2026]	Intelligence Community Directive 203: Analytic Standards	Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products.	original source-guide
[298, 2026]	Intelligence Community Directives	Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations.	original source-guide

Where this sits. This module's overview is Section 40; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

40.3.4 Soviet and Russian Intelligence governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 40; [266, 2026].

40.3.5 Soviet and Russian Intelligence analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 27's governance-boundary section, directly verified anchors for the **Historical and Declassified Intelligence Services** lane include [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]; [Archives and Administration, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Research lane: **Historical and Declassified Intelligence Services** for **Declassified source-protection and institutional-control case study; Declassified training-manual archive**. [266, 2026]; [267, 2026].
Curriculum topic spine: Declassified source-protection and institutional-control case study, **Declassified training-manual archive**, **Declassified source-protection and agent-handling ethics**. **Verified anchor cluster:** [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]; [Archives and Administration, 2026b]; [of the Director of National Intelligence, 2026e]; [Jr., 2007]; [Agency, 2009].
Conceptual depth: turning declassified records and official histories into safe institutional lessons about analytic judgment, secrecy, oversight, technical-intelligence evolution, and reform.
Method stack: provenance review, declassification-status notation, institutional timeline building, case-to-principle translation, and uncertainty about redacted records.
Composability contract: archive source, release channel, historical context, analytic lesson, oversight implication, and modern analogy remain explicitly separated.
Known failure modes: romanticized tradecraft, presentist interpretation, redaction overclaiming, decontextualized case reuse, and translating history into operational instructions.
Defensive boundary: historical modules use declassified or public records for analysis and governance lessons only; they do not reconstruct live tactics, sources, methods, or current field procedures. Applied to **Declassified source-protection and institutional-control case study; Declassified training-manual archive**.

Anchor	Why it matters here
[Agency, 2026a]	Official CSI landing page for Studies in Intelligence, declassified professional reflection, analytic history, and institutional learning. Checked as of 2026-05-21; role: curriculum_anchor.
[Agency, 2026h]	Official declassified historical-release library for cryptologic history, SIGINT history, COMSEC, oral histories, and historical cases. Checked as of 2026-05-21; role: curriculum_anchor.
[Office, 2026a]	Official declassified satellite-reconnaissance program archive for CORONA, GAMBIT, POPPY, QUILL, and other historical technical-intelligence cases. Checked as of 2026-05-21; role: curriculum_anchor.
[Archives and Administration, 2026b]	Official NARA guide to CIA Record Group 263, archival provenance, record series, and declassified intelligence research pathways. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026e]	Official ODNI explanation of analytic objectivity, ombuds, and tradecraft standards. Checked as of 2026-05-21; role: curriculum_anchor.
[Jr., 2007]	Foundational analytic cognition source for bias, mental models, and structured reasoning. Checked as of 2026-06-06; role: curriculum_anchor.
[Agency, 2009]	Official structured analytic techniques primer for bias checks, alternatives, and warning analysis. Checked as of 2026-05-21; role: curriculum_anchor.

40.3.5.1 Soviet and Russian Intelligence evidence standard and citation floor: source families and discovery limits Official guidance supplies governance, safety, and legal constraints for the **Historical and Declassified Intelligence Services** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [266, 2026]; [267, 2026].

40.3.6 Soviet and Russian Intelligence agentic boundary: assist, approve, block, and record

Evidence anchor. Section 40; [266, 2026].
AGEINT translation is bounded by the **Historical and Declassified Intelligence Services** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Declassified source-protection and institutional-control case study; Declassified training-manual archive**.

40.3.6.1 Soviet and Russian Intelligence permitted defensive utility: curriculum uses and safe outputs **Evidence anchor.** Section 40; [266, 2026].
The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Declassified source-protection and institutional-control case study; Declassified training-manual archive**.

40.3.6.2 Soviet and Russian Intelligence excluded operational boundary: blocked actions and stop rules Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [266, 2026]; [267, 2026] and **Declassified source-protection and institutional-control case study; Declassified training-manual archive**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

40.3.7 Soviet and Russian Intelligence governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 40; [266, 2026].
Governance is practiced as a gate on the **Historical and Declassified Intelligence Services** lane. Learners use the **Historical Case-Translation Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact

must stop for human review while using **Declassified source-protection and institutional-control case study; Declassified training-manual archive**.

40.3.7.1 Soviet and Russian Intelligence governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [266, 2026]; [267, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Historical and Declassified Intelligence Services** failure modes and the **Historical Case-Translation Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

40.3.7.2 Soviet and Russian Intelligence evidence package handoff: appendices, records, and reuse

Evidence anchor. Section 40; [266, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Historical Case-Translation Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Declassified source-protection and institutional-control case study; Declassified training-manual archive**.

40.3.7.3 Soviet and Russian Intelligence current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Declassified source-protection and institutional-control case study; Declassified training-manual archive**. [266, 2026]; [267, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_cia_center_for_study_of_intelligence` for **Declassified source-protection and institutional-control case study; Declassified training-manual archive**?	Center for the Study of Intelligence; lane `historical_declassified_sources`; checked 2026-05-21.	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary; Official CSI landing page for Studies in Intelligence, declassified professional reflection, analytic history, and institutional learning.
What does the module inherit from `official_nsa_historical_releases` for **Declassified source-protection and institutional-control case study; Declassified training-manual archive**?	NSA Historical Releases; lane `historical_declassified_sources`; checked 2026-05-21.	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary; Official declassified historical-release library for cryptologic history, SIGINT history, COMSEC, oral histories, and historical cases.
What does the module inherit from `official_nro_declassified_programs` for **Declassified source-protection and institutional-control case study; Declassified training-manual archive**?	Declassified NRO Programs and Projects; lane `historical_declassified_sources`; checked 2026-05-21.	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary; Official declassified satellite-reconnaissance program archive for CORONA, GAMBIT, POPPY, QUILL, and other historical technical-intelligence cases.
What does the module inherit from `official_nara_cia_records` for **Declassified source-protection and institutional-control case study; Declassified training-manual archive**?	Records of the Central Intelligence Agency; lane `historical_declassified_sources`; checked 2026-05-21.	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary; Official NARA guide to CIA Record Group 263, archival provenance, record series, and declassified intelligence research pathways.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 40; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

40.3.8 Soviet and Russian Intelligence assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 40; [266, 2026].

40.3.9 Soviet and Russian Intelligence assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 40; [266, 2026].

40.3.9.1 Soviet and Russian Intelligence capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Declassified source-protection and institutional-control case study; Declassified training-manual archive**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Declassified source-protection and institutional-control case study; Declassified training-manual archive** and [266, 2026]; [267, 2026].

40.3.9.2 Soviet and Russian Intelligence instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Declassified source-protection and institutional-control case study; Declassified training-manual archive**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Declassified source-protection and institutional-control case study; Declassified training-manual archive** and [266, 2026]; [267, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

40.3.9.3 Soviet and Russian Intelligence assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Declassified source-protection and institutional-control case study	Completed **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Declassified training-manual archive	Completed **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Declassified source-protection and agent-handling ethics	Completed **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Declassified source-protection and institutional-control case study; Declassified training-manual archive** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

40.3.10 Soviet and Russian Intelligence refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [266, 2026]; [267, 2026] and **Declassified source-protection and institutional-control case study; Declassified training-manual archive**.

40.3.10.1 Soviet and Russian Intelligence refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Declassified source-protection and institutional-control case study; Declassified training-manual archive**. The local signals begin with [266, 2026]; [267, 2026].

40.3.10.2 Soviet and Russian Intelligence claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Declassified source-protection and institutional-control case study; Declassified training-manual archive**, and the source spine for these checks begins with [266, 2026]; [267, 2026].

40.3.11 Soviet and Russian Intelligence reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [266, 2026]; [267, 2026].

Triangulation anchors. In module 27's review-checklist section, directly verified anchors for the **Historical and Declassified Intelligence Services** lane include [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]; [Archives and Administration, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Declassified source-protection and institutional-control case study; Declassified training-manual archive**. [266, 2026]; [267, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

40.3.12 Soviet and Russian Intelligence learning-path links: module map, overview, and curriculum atlas

These links keep **Declassified source-protection and institutional-control case study; Declassified training-manual archive** paired with the orientation atlas, the parent unit, and the previous and next modules, so a reader can trace which claims and caveats are inherited rather than re-derived here. Anchored at [266, 2026]; [267, 2026].

Section 2, Section 39, Section 41

41 American Intelligence History

41.0.1 American Intelligence History figures and course links: visual evidence, source flow, and navigation

The module uses Figure 82 and Figure 79 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 39, Section 40, Section 42.
This module teaches the **Historical and Declassified Intelligence Services** lane through a bounded, source-backed coursebook chapter. [266, 2026]; [269, 2026].

41.1 Historical and Declassified Intelligence Services frame for American Intelligence History: source context, topic focus, and reader task

Evidence anchor. Section 41; [266, 2026].

41.1.1 American Intelligence History orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 41; [266, 2026].

41.1.2 American Intelligence History conceptual primer: source context, core model, and reader task

This chapter teaches historical intelligence study as declassified evidence review: archives teach institutional lessons when provenance, redaction, context, and modern boundaries are explicit. The chapter uses **Historical Case-Translation Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**.
The central distinction is to separate historical lesson from reconstruction of live tactics or current sources and methods. Core topics include **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study; OSS Provisional Basic Field Manual: Declassified source-protection and institutional-control case study**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [266, 2026]; [269, 2026].
Learners move from vocabulary and the **Historical Case-Translation Lens** distinction through topic lessons on **Declassified source-protection and institutional-control case study** with evidence and misconception checks, then assemble a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** with safety and rights gates.

41.1.3 American Intelligence History learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 41; [266, 2026].

- Connect **Declassified source-protection and institutional-control case study and OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study** to **Historical and Declassified Intelligence Services** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate historical lesson from reconstruction of live tactics or current sources and methods; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as romanticized tradecraft, presentist interpretation, redaction overclaiming, decontextualized case reuse, and translating history into operational instructions, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: historical modules use declassified or public records for analysis and governance lessons only; they do not reconstruct live tactics, sources, methods, or current field procedures.

41.1.4 American Intelligence History core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 41; [266, 2026].

Term	Working definition
Declassification context	the release channel, date, and limits of an official historical source
Redaction caveat	the warning that missing text may change interpretation
Institutional lesson	the durable governance or analytic principle drawn from a case
Presentism	the error of forcing modern assumptions onto a historical record
Modern analogy	a bounded comparison that preserves differences between eras
Oversight failure	a documented breakdown in review, records, or accountability visible in the archive
Source-protection lesson	the historical principle about protecting people and methods without reconstructing live tradecraft
Declassified source-protection and…	Key terms: Declassified, protection, institutional.
OSS Secret Intelligence Manual: Declassified…	Key terms: OSS, Secret, Manual.

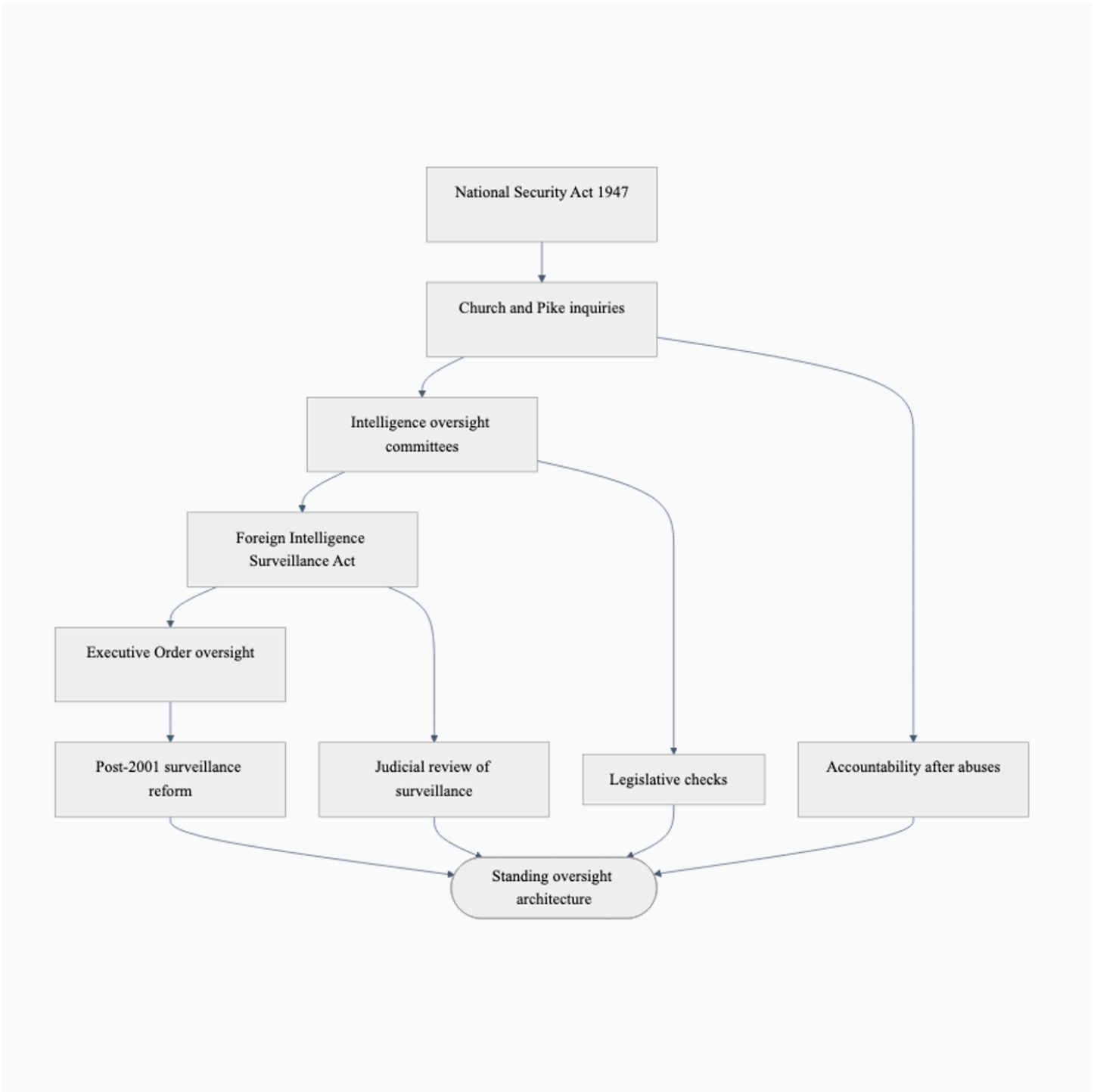


Figure 82: A milestone view of how American intelligence accountability was progressively built through founding statutes, investigations, oversight committees, and surveillance-law reform. Its reader value is to make National Security Act 1947, Church and Pike inquiries, Intelligence oversight committees, and Foreign Intelligence Surveillance Act visible at a glance, with the historical intelligence services / american intelligence history section as the source section and defensive review as the boundary.

41.2 Historical Case-Translation Lens path for American Intelligence History: lesson cluster, safe artifact, and review

Evidence anchor. Section 41; [266, 2026].

41.2.1 American Intelligence History practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 41; [266, 2026].

41.2.2 American Intelligence History topic lessons: source-backed concepts and transfer tasks

This module builds historical intelligence study as declassified evidence review: archives teach institutional lessons when provenance, redaction, context, and modern boundaries are explicit. The sequence opens with **Declassified source-protection and institutional-control case study**, **OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**, **OSS Provisional Basic Field Manual: Declassified source-protection and institutional-control case study** and applies the **Historical Case-Translation Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 79; module overview Section 41; curriculum atlas Section 2.

Triangulation anchors. In module 28's topic-lessons section, directly verified anchors for the **Historical and Declassified Intelligence Services** lane include [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]; [Archives and Administration, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

41.2.2.1 Lesson 1: Declassified source-protection and institutional-control case study

Concept. Declassified source-protection and institutional-control case study studies OSS declassified manuals for oversight, ethics, and limits on translating history into practice.

Why it matters. Declassified source-protection matters in the **Historical and Declassified Intelligence Services** lane because declassified-source interpretation and case-to-principle translation evidence must stay separate from judgment; romanticized tradecraft is a common failure.

Source support. Declassified source-protection and institutional-control case study rests on [128, 2026] and [129, 2026]. Its anchor reference records: The page functions as a curated library of links to external sites covering OSS history, including operations, related organizations, notable figures such as William Donovan and Allen Dulles, educational materials, and geographic theaters. Use them for the working definition that **Declassified source-protection and institutional-control case study** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. For **Declassified source-protection**, work from the cited evidence behind this row. [128, 2026] An Internet Archive full-text scan of the proceedings of a 1991 National Archives conference on the Office of Strategic Services (OSS), the U.S. [129, 2026] A resource directory page from the Office of Strategic Services Society, a historical organization dedicated to preserving the record of the WWII-era OSS. The page functions as a curated library of links to external sites covering OSS history, including operations, related organizations, notable figures such as William Donovan and Allen Dulles, educational materials, and geographic theaters. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Declassified source-protection**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **Declassified source-protection and institutional-control case**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape **Declassified source-protection** work as a **declassified case-to-principle card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Reuse the **Declassified source-protection** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

41.2.2.2 Lesson 2: OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study

Concept. OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study studies OSS declassified manuals for oversight, ethics, and limits on translating history into practice.

Why it matters. Analysts use **OSS Secret Intelligence Manual** to separate historical lesson from reconstruction of live tactics or current sources and methods. A defensible treatment names the judgment it enables for declassified-source interpretation and case-to-principle translation review, the proof limit that romanticized tradecraft would otherwise hide, and the reviewer accountable for challenge.

Source support. OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study rests on [117, 2026]. The closest source to this row notes: The OSS was the WWII predecessor to the CIA, and the documents illustrate how the United States organized clandestine activities in occupied Europe and Asia. Use it for pinning down the scope of **OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. Read **OSS Secret Intelligence Manual** against the works cited for this row. [117, 2026] An article from Small Wars Journal (affiliated with Arizona State University) announcing that The Resistance Hub has compiled declassified Office of Strategic Services (OSS) manuals for public access. The OSS was the WWII predecessor to the CIA, and the documents illustrate how the United States organized clandestine activities in occupied Europe and Asia. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **OSS Secret Intelligence Manual**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **OSS Secret Intelligence Manual**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape **OSS Secret Intelligence Manual** work as a **declassified case-to-principle card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Reuse the **OSS Secret Intelligence Manual** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

41.2.2.3 Lesson 3: OSS Provisional Basic Field Manual: Declassified source-protection and institutional-control case study

Concept. OSS Provisional Basic Field Manual: Declassified source-protection and institutional-control case study studies OSS declassified manuals for oversight, ethics, and limits on translating history into practice.

Why it matters. Without explicit treatment of **OSS Provisional Basic Field Manual**, romanticized tradecraft undermines declassified-source interpretation and case-to-principle translation review; the lesson builds the habit to separate historical lesson from reconstruction of live tactics or current sources and methods.

Source support. OSS Provisional Basic Field Manual: Declassified source-protection and institutional-control case study rests on [119, 2026]. Use it for pinning down the scope of **OSS Provisional Basic Field Manual: Declassified source-protection and institutional-control case study**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. Read **OSS Provisional Basic Field Manual** against the works cited for this row. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **OSS Provisional Basic Field Manual**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **OSS Provisional Basic Field Manual**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape **OSS Provisional Basic Field Manual** work as a **declassified case-to-principle card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Reuse the **OSS Provisional Basic Field Manual** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

41.2.2.4 Lesson 4: Hybrid-threat indicator review using sample scenarios and policy thresholds

Concept. Hybrid-threat indicator review using sample scenarios and policy thresholds reads special-operations intelligence as support to accountable planning with explicit authority and oversight fields.

Why it matters. Hybrid-threat indicator review connects classroom vocabulary to Historical and Declassified Intelligence Services practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Hybrid-threat indicator review using sample scenarios and policy thresholds rests on [118, 2026]. The closest source to this row notes: The 32-page manual sets out the authorized functions, operational plans, methods, and organization of OSS Maritime Units and the broader Special Operations Branch. Use it for pinning down the scope of **Hybrid-threat indicator review using sample scenarios and policy thresholds**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. For **Hybrid-threat indicator review**, work from the cited evidence behind this row. [118, 2026] A digitized World War II field manual from the Internet Archive, the Special Operations Field Manual, Strategic Services (provisional), issued July 18, 1944 by the U.S. Office of Strategic Services (OSS). The 32-page manual sets out the authorized functions, operational plans, methods, and organization of OSS Maritime Units and the broader Special Operations Branch. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Hybrid-threat indicator review**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must name the indicator descriptor, the bounded claim about **Hybrid-threat indicator review using sample**, the attribution caveat, the threshold uncertainty, the non-attribution boundary, and the reviewer who approves the policy read. Shape **Hybrid-threat indicator review** work as a **declassified case-to-principle card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Hybrid-threat indicator review**: that activity falling below an obvious threshold is therefore ungoverned, rather than still bound by escalation limits and accountable review.

Transfer task. Apply this module's safe boundary for **Hybrid-threat indicator review** to another artifact while keeping declassified-source interpretation and case-to-principle translation and reviewer ownership explicit.

41.2.2.5 Lesson 5: OSS Special Weapons and Devices: Declassified source-protection and institutional-control case study

Concept. OSS Special Weapons and Devices: Declassified source-protection and institutional-control case study studies OSS declassified manuals for oversight, ethics, and limits on translating history into practice.

Why it matters. OSS Special Weapons and Devices matters in the **Historical and Declassified Intelligence Services** lane because declassified-source interpretation and case-to-principle translation evidence must stay separate from judgment; romanticized tradecraft is a common failure.

Source support. OSS Special Weapons and Devices: Declassified source-protection and institutional-control case study rests on [117, 2026]. The most specific cited work observes: The OSS was the WWII predecessor to the CIA, and the documents illustrate how the United States organized clandestine activities in occupied Europe and Asia. Use it for the working definition that **OSS Special Weapons and Devices: Declassified source-protection and institutional-control case study** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. Read **OSS Special Weapons and Devices** against the works cited for this row. [117, 2026] An article from Small Wars Journal (affiliated with Arizona State University) announcing that The Resistance Hub has compiled declassified Office of Strategic Services (OSS) manuals for public access. The OSS was the WWII predecessor to the CIA, and the documents illustrate how the United States organized clandestine activities in occupied Europe and Asia. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **OSS Special Weapons and Devices**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **OSS Special Weapons and Devices**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape **OSS Special Weapons and Devices** work as a **declassified case-to-principle card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Apply this module's safe boundary for **OSS Special Weapons and Devices** to another artifact while keeping declassified-source interpretation and case-to-principle translation and reviewer ownership explicit.

41.2.2.6 Lesson 6: Simple Sabotage Field Manual: Declassified source-protection and institutional-control case study

Concept. Simple Sabotage Field Manual: Declassified source-protection and institutional-control case study studies OSS declassified manuals for oversight, ethics, and limits on translating history into practice.

Why it matters. Without explicit treatment of **Simple Sabotage Field Manual**, romanticized tradecraft undermines declassified-source interpretation and case-to-principle translation review; the lesson builds the habit to separate historical lesson from reconstruction of live tactics or current sources and methods.

Source support. Simple Sabotage Field Manual: Declassified source-protection and institutional-control case study rests on [117, 2026]. Its anchor reference records: An article from Small Wars Journal (affiliated with Arizona State University) announcing that The Resistance Hub has compiled declassified Office of Strategic Services (OSS) manuals for public access. Use it for fixing what **Simple Sabotage Field Manual: Declassified source-protection and institutional-control case study** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. For **Simple Sabotage Field Manual**, work from the cited evidence behind this row. [117, 2026] An article from Small Wars Journal (affiliated with Arizona State University) announcing that The Resistance Hub has compiled declassified Office of Strategic Services (OSS) manuals for public access. The OSS was the WWII predecessor to the CIA, and the documents illustrate how the United States organized clandestine activities in occupied Europe and Asia. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Simple Sabotage Field Manual**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **Simple Sabotage Field Manual**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape **Simple Sabotage Field Manual** work as a **declassified case-to-principle card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Transfer **Simple Sabotage Field Manual** from this module to a second motif by preserving declassified-source interpretation and case-to-principle translation, replacing action with audit, and naming the blocked use.

41.2.2.7 Lesson 7: Morale Operations Field Manual: Declassified source-protection and institutional-control case study

Concept. Morale Operations Field Manual: Declassified source-protection and institutional-control case study studies OSS declassified manuals for oversight, ethics, and limits on translating history into practice.

Why it matters. Morale Operations Field Manual matters in the **Historical and Declassified Intelligence Services** lane because declassified-source interpretation and case-to-principle translation evidence must stay separate from judgment; romanticized tradecraft is a common failure.

Source support. Morale Operations Field Manual: Declassified source-protection and institutional-control case study rests on [117, 2026]. Its anchor reference records: The OSS was the WWII predecessor to the CIA, and the documents illustrate how the United States organized clandestine activities in occupied Europe and Asia. Use it for pinning down the scope of **Morale Operations Field Manual: Declassified source-protection and institutional-control case study**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. Ground **Morale Operations Field Manual** in the evidence the row cites. [117, 2026] An article from Small Wars Journal (affiliated with Arizona State University) announcing that The Resistance Hub has compiled declassified Office of Strategic Services (OSS) manuals for public access. The OSS was the WWII predecessor to the CIA, and the documents illustrate how the United States organized clandestine activities in occupied Europe and Asia. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Morale Operations Field Manual**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **Morale Operations Field Manual**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape **Morale Operations Field Manual** work as a **declassified case-to-principle card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Transfer **Morale Operations Field Manual** from this module to a second motif by preserving declassified-source interpretation and case-to-principle translation, replacing action with audit, and naming the blocked use.

41.2.2.8 Lesson 8: CIA Cold War Operations: Declassified source-protection and institutional-control case study

Concept. CIA Cold War Operations: Declassified source-protection and institutional-control case study studies the declassified record for institutional lessons about oversight, source protection, and limits on translating history into practice.

Why it matters. Analysts use **CIA Cold War Operations** to separate historical lesson from reconstruction of live tactics or current sources and methods. A defensible treatment names the judgment it enables for declassified-source interpretation and case-to-principle translation review, the proof limit that romanticized tradecraft would otherwise hide, and the reviewer accountable for challenge.

Source support. CIA Cold War Operations: Declassified source-protection and institutional-control case study rests on [297, 2026] and [298, 2026]. The closest source to this row notes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for fixing what **CIA Cold War Operations: Declassified source-protection and institutional-control case study** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. Ground **CIA Cold War Operations** in the evidence the row cites. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **CIA Cold War Operations**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **CIA Cold War Operations**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape **CIA Cold War Operations** work as a **declassified case-to-principle card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Transfer **CIA Cold War Operations** from this module to a second motif by preserving declassified-source interpretation and case-to-principle translation, replacing action with audit, and naming the blocked use.

41.2.2.9 Lesson 9: CIA Manual of Trickery and: Declassified source-protection and institutional-control case study

Concept. CIA Manual of Trickery and: Declassified source-protection and institutional-control case study compares deception indicators with alternative explanations and uncertainty before any operational inference.

Why it matters. Without explicit treatment of **CIA Manual of Trickery and**, romanticized tradecraft undermines declassified-source interpretation and case-to-principle translation review; the lesson builds the habit to separate historical lesson from reconstruction of live tactics or current sources and methods.

Source support. CIA Manual of Trickery and: Declassified source-protection and institutional-control case study rests on [130, 2026]. Its anchor reference records: A reproduction of a Cold War-era manual written by magician John Mulholland for the CIA, presented with commentary by H. Use it for fixing what **CIA Manual of Trickery and: Declassified source-protection and institutional-control case study** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. For **CIA Manual of Trickery and**, reason from the sources cited in this row. [130, 2026] A reproduction of a Cold War-era manual written by magician John Mulholland for the CIA, presented with commentary by H. Keith Melton and Robert Wallace as "The Official CIA

Manual of Trickery and Deception." The book situates the manual within the history of the MKULTRA program and the long-missing magic manuals, and reproduces Mulholland's guidance on applying sleight-of-hand and misdirection techniques to covert operational tasks. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **CIA Manual of Trickery and**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **CIA Manual of Trickery**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape **CIA Manual of Trickery and** work as a **declassified case-to-principle card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Reuse the **CIA Manual of Trickery and** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

41.2.2.10 Lesson 10: Principles of Tradecraft: Declassified source-protection and institutional-control case study

Concept. Principles of Tradecraft: Declassified source-protection and institutional-control case study studies the declassified record for institutional lessons about source protection, oversight, and the danger of translating historical methods into current practice.

Why it matters. Principles of Tradecraft matters in the **Historical and Declassified Intelligence Services** lane because declassified-source interpretation and case-to-principle translation evidence must stay separate from judgment; romanticized tradecraft is a common failure.

Source support. Principles of Tradecraft: Declassified source-protection and institutional-control case study rests on [120, 2026]. Its anchor reference records: Principles of Tradecraft, a 1995 publication by Militia Free Press (a subsidiary of The Resister). Use it for pinning down the scope of **Principles of Tradecraft: Declassified source-protection and institutional-control case study**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. Read **Principles of Tradecraft** against the works cited for this row. [120, 2026] Principles of Tradecraft, a 1995 publication by Militia Free Press (a subsidiary of The Resister). The document presents an overview of intelligence and espionage concepts, with chapters covering an introduction to espionage, agents (typology, identification, recruitment, and handling), and agent organization and management including personnel and structures. It is framed as an introductory treatment rather than a comprehensive reference on intelligence requirements. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Principles of Tradecraft**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **Principles of Tradecraft**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape **Principles of Tradecraft** work as a **declassified case-to-principle card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Transfer **Principles of Tradecraft** from this module to a second motif by preserving declassified-source interpretation and case-to-principle translation, replacing action with audit, and naming the blocked use.

41.2.2.11 Lesson 11: Cognitive influence-analysis case review using sample materials

Concept. Cognitive influence-analysis case review using sample materials analyzes influence campaigns through provenance, audience harm, attribution caution, and transparent response options.

Why it matters. Without explicit treatment of **Cognitive influence-analysis case review**, treating resilience labels as permission to skip provenance review undermines declassified-source interpretation and case-to-principle translation review; the lesson builds the habit to separate historical lesson from reconstruction of live tactics or current sources and methods.

Source support. Cognitive influence-analysis case review using sample materials rests on [088, 2026], [089, 2026], and [090, 2026]. The most specific cited work observes: A U.S. Use them for the claim that **Cognitive influence-analysis case review using sample materials** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. Read **Cognitive influence-analysis case review** against the works cited for this row. [088, 2026] A U.S. Department of State Bureau of Public Affairs report from October 1981, released under FOIA. It catalogs Soviet 'active measures' — the Soviet term for covert influence operations — including written disinformation, control of foreign media, use of front organizations, clandestine broadcasting, blackmail, and political influence operations. Specific cases include Soviet forgeries related to the 1979 Grand Mosque seizure and NATO theater nuclear force debates. [089, 2026] An article by Dennis Kux published in Parameters: Journal of the US Army War College (1985) and preserved in the CIA CREST archive. It defines and distinguishes Soviet 'disinformation' and 'active measures,' situating them within a spectrum of white, gray, and black foreign influence operations. Kux examines KGB front groups, agents of influence, forgeries, and the broader strategic goal of tarnishing Western governments while advancing Soviet foreign policy. [090, 2026] A CIA CREST record (October 1981, released March 2007) comprising a routing and record sheet from the PCS/PGLO office dated February 8, 1982, attached to the same Department of State Special Report No. 88 on Soviet active measures. The document is catalogued as an open-source CREST entry and captures the internal CIA circulation of the State Department's public report on Soviet forgery and disinformation operations. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Cognitive influence-analysis case review**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must record the narrative provenance, the bounded claim about **Cognitive influence-analysis case review using**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Cognitive influence-analysis case review** work as a **declassified case-to-principle card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Cognitive influence-analysis case review**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Apply this module's safe boundary for **Cognitive influence-analysis case review** to another artifact while keeping declassified-source interpretation and case-to-principle translation and reviewer ownership explicit.

41.2.2.12 Lesson 12: Studies in Intelligence: Declassified source-protection and institutional-control case study

Concept. Studies in Intelligence: Declassified source-protection and institutional-control case study studies the declassified record for institutional lessons about oversight, source protection, and limits on translating history into practice.

Why it matters. Studies in Intelligence matters in the **Historical and Declassified Intelligence Services** lane because declassified-source interpretation and case-to-principle translation evidence must stay separate from judgment; romanticized tradecraft is a common failure.

Source support. Studies in Intelligence: Declassified source-protection and institutional-control case study rests on [131, 2026], [132, 2026], and [133, 2026]. The most specific cited work observes: Studies in Intelligence is the CIA's professional journal, published by the Center for the Study of Intelligence (CSI). Use them for the claim that **Studies in Intelligence: Declassified source-protection and institutional-control case study** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. Ground **Studies in Intelligence** in the evidence the row cites. [131, 2026] The Center for the Study of Intelligence (CSI) serves as a producer and repository of unclassified. [132, 2026] Studies in Intelligence is the CIA's professional journal, published by the Center for the Study of Intelligence (CSI). It covers historical, analytical, and methodological topics across the intelligence profession, and is issued quarterly in partially declassified extract form. As of 2026 the archive holds 110 issues, with the most recent being Volume 70, No. 1 (March 2026); articles are written by intelligence community professionals under their own names or pen names. [133, 2026] This is a National Security Archive briefing book presenting declassified articles from the CIA's internal journal Studies in Intelligence, first published in 1955. The collection gathers articles obtained through Freedom of Information Act requests and litigation, spanning CIA history from the Kennedy era through the post-9/11 period. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Studies in Intelligence**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **Studies in Intelligence**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape **Studies in Intelligence** work as a **declassified case-to-principle card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Transfer **Studies in Intelligence** from this module to a second motif by preserving declassified-source interpretation and case-to-principle translation, replacing action with audit, and naming the blocked use.

41.2.2.13 Lesson 13: Declassified source-protection and institutional-control case study (28.3.1)

Concept. Declassified source-protection and institutional-control case study (28.3.1) studies the declassified record for institutional lessons about source protection, oversight, and the danger of translating historical methods into current practice.

Why it matters. Analysts use **Declassified source-protection** to separate historical lesson from reconstruction of live tactics or current sources and methods. A defensible treatment names the judgment it enables for declassified-source interpretation and case-to-principle translation review, the proof limit that romanticized tradecraft would otherwise hide, and the reviewer accountable for challenge.

Source support. Declassified source-protection and institutional-control case study (28.3.1) rests on [019, 2026] and [034, 2026]. Its anchor reference records: By Thomas Mulligan, a researcher at the RAND Corporation who served in CIA during 2008–14. Use them for the claim that **Declassified source-protection and institutional-control case study (28.3.1)** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. For **Declassified source-protection**, work from the cited evidence behind this row. [019, 2026] By Thomas Mulligan, a researcher at the RAND Corporation who served in CIA during 2008–14. [034, 2026] Thomas Mulligan is a researcher at the RAND Corporation and former CIA officer. Ana P. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Declassified source-protection**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **Declassified source-protection and institutional-control case**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape **Declassified source-protection** work as a **declassified case-to-principle card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Apply this module's safe boundary for **Declassified source-protection** to another artifact while keeping declassified-source interpretation and case-to-principle translation and reviewer ownership explicit.

41.2.2.14 Lesson 14: Declassified source-protection and institutional-control case study (28.3.2)

Concept. Declassified source-protection and institutional-control case study (28.3.2) treats open sources as publicly available evidence that still requires provenance, corroboration, legality, and minimization before reuse.

Why it matters. Declassified source-protection matters in the **Historical and Declassified Intelligence Services** lane because declassified-source interpretation and case-to-principle translation evidence must stay separate from judgment; romanticized tradecraft is a common failure.

Source support. Declassified source-protection and institutional-control case study (28.3.2) rests on [047, 2026]. The lead source's own note reads: Plans and strategies for improving open-source intelligence (OSINT) operations in the Intelligence. Use it for fixing what **Declassified source-protection and institutional-control case study (28.3.2)** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. For **Declassified source-protection**, work from the cited evidence behind this row. [047, 2026] Plans and strategies for improving open-source intelligence (OSINT) operations in the Intelligence. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Declassified source-protection**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **Declassified source-protection and institutional-control case**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape **Declassified source-protection** work as a **declassified case-to-principle card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Transfer **Declassified source-protection** from this module to a second motif by preserving declassified-source interpretation and case-to-principle translation, replacing action with audit, and naming the blocked use.

41.2.2.15 Lesson 15: History of SIGINT at the: Declassified source-protection and institutional-control case study

Concept. History of SIGINT at the: Declassified source-protection and institutional-control case study frames SIGINT as authority-bound collection with minimization, handling rules, and communications-security implications.

Why it matters. History of SIGINT at the connects classroom vocabulary to Historical and Declassified Intelligence Services practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. History of SIGINT at the: Declassified source-protection and institutional-control case study rests on [038, 2026] and [039, 2026]. The closest source to this row notes: A 2015 briefing book from the National Security Archive, compiled by Jeffrey T. Use them for the working definition that **History of SIGINT at the: Declassified source-protection and institutional-control case study** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. Ground **History of SIGINT at the** in the evidence the row cites. [038, 2026] A January 2018 blog post on Open INT recounting the CIA's role in signals intelligence from roughly 1947 to 1970, noting that SIGINT is often associated with the NSA but the CIA also participated. It distinguishes communications intelligence from electronic intelligence and references declassified Cold War operations including U-2 collection and a Berlin communications-tapping effort. [039, 2026] A 2015 briefing book from the National Security Archive, compiled by Jeffrey T. Richelson, presenting declassified documents on the CIA's signals intelligence activities from roughly 1947 to 1970. It documents the CIA's parallel

SIGINT operations alongside the NSA during the Cold War, covering programs and collection efforts as well as recurring friction between the two agencies over mission overlap, budgets, and access to intelligence. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **History of SIGINT at the**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **History of SIGINT**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape **History of SIGINT at the** work as a **declassified case-to-principle card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Transfer **History of SIGINT at the** from this module to a second motif by preserving declassified-source interpretation and case-to-principle translation, replacing action with audit, and naming the blocked use.

41.2.2.16 Lesson 16: NSA WWII Declassified: Declassified source-protection and institutional-control case study

Concept. NSA WWII Declassified: Declassified source-protection and institutional-control case study frames SIGINT as authority-bound collection with minimization, handling rules, and communications-security implications.

Why it matters. NSA WWII Declassified connects classroom vocabulary to Historical and Declassified Intelligence Services practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. NSA WWII Declassified: Declassified source-protection and institutional-control case study rests on [036, 2026]. The lead source's own note reads: Volumes 1 - 9 of the European Axis Signal Intelligence in WWII documentation. Use it for fixing what **NSA WWII Declassified: Declassified source-protection and institutional-control case study** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. Ground **NSA WWII Declassified** in the evidence the row cites. [036, 2026] Volumes 1 - 9 of the European Axis Signal Intelligence in WWII documentation. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **NSA WWII Declassified**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **NSA WWII Declassified**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape **NSA WWII Declassified** work as a **declassified case-to-principle card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Transfer **NSA WWII Declassified** from this module to a second motif by preserving declassified-source interpretation and case-to-principle translation, replacing action with audit, and naming the blocked use.

41.2.3 American Intelligence History worked safe example: synthetic inputs, evidence, and review

Worked example: a sample seminar studies a declassified reform episode and extracts an oversight lesson without reconstructing current sources and methods. [266, 2026]; [269, 2026].

Triangulation anchors. In module 28's worked-example section, directly verified anchors for the **Historical and Declassified Intelligence Services** lane include [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]; [Archives and Administration, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **declassified-source interpretation**. Learners use a **declassified case-to-principle card** and keep this boundary visible: No current sources-and-methods reconstruction, operational emulation, or tactical transfer.

Frame. The classroom question centers on **Declassified source-protection and institutional-control case study**. Excluded actions stay explicit, and the **Historical Case-Translation Lens** planning question is: Which declassified source, release context, institutional lesson, and modern boundary can be carried forward without recreating operations?

Inputs. For the **Declassified source-protection and institutional-control case study** scenario, use public archive metadata, a short excerpt, a timeline template, and an oversight-question worksheet. The Historical Case-Translation Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Declassified source-protection and institutional-control case study**, students record provenance, mark redactions, build timeline, distinguish known from unknown, and extract a governance lesson. Pause whenever an inference about Declassified source-protection and institutional-control case study appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Declassified source-protection and institutional-control case study** classroom scenario; unit artifact = declassified case-to-principle card; evidence = allowed inputs; method = declassified-source interpretation and case-to-principle translation; output = a historical case card with release context, caveats, lesson, and evidence-bounded boundary; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Declassified source-protection and institutional-control case study** as "Historical Case-Translation Lens confirms it" is not enough. The revision ties the claim to declassified-source interpretation and case-to-principle translation, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Declassified source-protection and institutional-control case study** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

41.2.4 American Intelligence History practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Historical Case-Translation Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**.

Triangulation anchors. In module 28's practice-sequence section, directly verified anchors for the **Historical and Declassified Intelligence Services** lane include [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]; [Archives and Administration, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Declassified source-protection and institutional-control case study, OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study, OSS Provisional Basic Field Manual: Declassified source-protection and institutional-control case study; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Historical and Declassified Intelligence Services** lane.
2. Frame	Answer the lens question: Which declassified source, release context, institutional lesson, and modern boundary can be carried forward without recreating operations?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Declassified source-protection and institutional-control case study: historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the declassified case-to-principle card fields for Declassified source-protection and institutional-control case study.	Unit profile note.	Evidence artifacts include release metadata, redaction caveat.
4. Challenge	Test the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.	Failure-mode note.	The artifact applies the key distinction: separate historical lesson from reconstruction of live tactics or current sources and methods.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

41.2.4.1 American Intelligence History instructor notes: source reasoning, review points, and studio focus Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**. [266, 2026]; [269, 2026].

41.2.4.2 American Intelligence History extension exercise: peer validation and refresh trigger review **Evidence anchor.** Section 41; [266, 2026].

Have learners swap artifacts and apply the **Historical Case-Translation Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**.

41.2.5 American Intelligence History knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 41; [266, 2026].

1. Explain how **Declassified source-protection and institutional-control case study** is defined here; name the source descriptor that supports the definition.
2. Contrast **Declassified source-protection and institutional-control case study** with **OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study** using the **Historical Case-Translation Lens** artifact fields.
3. Identify one failure mode from the **Historical and Declassified Intelligence Services** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which institutional lesson is defensible from the record, and which claim reconstructs live tradecraft?
5. Correct this misconception: that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

41.2.5.1 American Intelligence History answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Declassified source-protection and institutional-control case study** without source evidence, uncertainty, or a safe transfer task.

41.3 American Intelligence History assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 41; [266, 2026].

41.3.1 American Intelligence History evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 41; [266, 2026].

41.3.2 American Intelligence History transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 41; [266, 2026].

41.3.2.1 American Intelligence History lineage and source tradition: profile, concepts, and first anchors This sits in the **Historical and Declassified Intelligence Services** lineage: turning declassified records and official histories into safe institutional lessons about analytic judgment, secrecy, oversight, technical-intelligence evolution, and reform. [266, 2026]; [269, 2026].

41.3.2.2 American Intelligence History working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 41; [266, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**, with provenance and reviewability throughout.

41.3.2.3 American Intelligence History knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [266, 2026]; [269, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

41.3.2.4 American Intelligence History transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 41; [266, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**.
- **Evidence contract:** keep the **Historical and Declassified Intelligence Services** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

41.3.2.5 American Intelligence History profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 41; [266, 2026].

The matched profile emphasizes turning declassified records and official histories into safe institutional lessons about analytic judgment, secrecy, oversight, technical-intelligence evolution, and reform. The method stack is provenance review, declassification-status notation, institutional timeline building, case-to-principle translation, and uncertainty about redacted records; the local topic cluster is **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**.

41.3.3 American Intelligence History evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 41; [266, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Historical and Declassified Intelligence Services** profile tells reviewers what evidence is strong enough for the module artifact built around **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**.

41.3.3.1 American Intelligence History guide source spine: inherited keys and local citation roles Primary guide citations: [266, 2026]; [269, 2026]; [271, 2026]; [280, 2026]; [281, 2026]; [282, 2026]; [292, 2026]; [295, 2026]; [296, 2026]; [128, 2026]; [129, 2026]; [117, 2026]; [119, 2026]; [118, 2026]; [130, 2026]; [120, 2026]; [088, 2026]; [089, 2026]; [090, 2026]; [091, 2026]; [131, 2026]; [132, 2026]; [133, 2026]; [019, 2026]; [034, 2026]; [047, 2026]; [038, 2026]; [039, 2026]; [036, 2026]; [297, 2026]; [298, 2026].

41.3.3.2 American Intelligence History verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [266, 2026]; [269, 2026].

Tier	What counts	How it is used
Source guide	[266, 2026]; [269, 2026]; [271, 2026]; [280, 2026]; [281, 2026]; [282, 2026]; [292, 2026]; [295, 2026]; [296, 2026]; [128, 2026]; [129, 2026]; [117, 2026]; [119, 2026]; [118, 2026]; [130, 2026]; [120, 2026]; [088, 2026]; [089, 2026]; [090, 2026]; [091, 2026]; [131, 2026]; [132, 2026]; [133, 2026]; [019, 2026]; [034, 2026]; [047, 2026]; [038, 2026]; [039, 2026]; [036, 2026]; [297, 2026]; [298, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 28's source-canon section, directly verified anchors for the **Historical and Declassified Intelligence Services** lane include [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]; [Archives and Administration, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study** and [266, 2026]; [269, 2026], but only directly verified source URLs are encoded as citations.

41.3.3.3 American Intelligence History intelligence practice lens: evidence artifact and safety check

Practice lens: **Historical Case-Translation Lens** for **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**. [266, 2026]; [269, 2026].

Planning question: Which declassified source, release context, institutional lesson, and modern boundary can be carried forward without recreating operations?

Evidence artifact: historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary.

Validation rule: distinguish what the record shows, what remains redacted or unknown, and which governance lesson is defensibly transferable. Applied to **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**.

Handoff contract: handoff preserves archive citation, historical context, analytic lesson, oversight implication, and modern analogy as separate fields.

Safety check: exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material.

41.3.3.4 American Intelligence History runtime-to-reader map: generated sections and verifier surfaces

Evidence anchor. Section 41; [266, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	28.99	28.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind American Intelligence History to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Bounded autonomy, procurement, incident-response, and assurance studio	28.101	28.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for American Intelligence History	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Model-card, recoverability, retention, and learner-support evidence package	28.102	28.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for American Intelligence History	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Declassified source-protection and institutional-control case study	28.1	28.1 source title transformed into safe curriculum treatment; original: OSS in World War II	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified source-protection and institutional-control case study	28.1.1	28.1.1 source title transformed into safe curriculum treatment; original: OSS Secret Intelligence Manual	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified source-protection and institutional-control case study	28.1.2	28.1.2 source title transformed into safe curriculum treatment; original: OSS Provisional Basic Field Manual	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Hybrid-threat indicator review using sample scenarios and policy thresholds	28.1.3	28.1.3 source title transformed into safe curriculum treatment; original: Special Operations Field Manual	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified source-protection and institutional-control case study	28.1.4	28.1.4 source title transformed into safe curriculum treatment; original: OSS Special Weapons and Devices	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified source-protection and institutional-control case study	28.1.5	28.1.5 source title transformed into safe curriculum treatment; original: Simple Sabotage Field Manual (1944)	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified source-protection and institutional-control case study	28.1.6	28.1.6 source title transformed into safe curriculum treatment; original: Morale Operations Field Manual	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified source-protection and institutional-control case study	28.2	28.2 source title transformed into safe curriculum treatment; original: CIA Cold War Operations	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified source-protection and institutional-control case study	28.2.1	28.2.1 source title transformed into safe curriculum treatment; original: CIA Manual of Trickery and Deception (Mulholland)	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified source-protection and institutional-control case study	28.2.2	28.2.2 source title transformed into safe curriculum treatment; original: Principles of Tradecraft (Resistance Operations)	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Cognitive influence-analysis case review using sample materials	28.2.3	28.2.3 source title transformed into safe curriculum treatment; original: Soviet Active Measures Documents (CREST Collection)	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Declassified source-protection and institutional-control case study	28.3	28.3 source title transformed into safe curriculum treatment; original: Studies in Intelligence: The CIA's Professional Journal	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified source-protection and institutional-control case study	28.3.1	28.3.1 source title transformed into safe curriculum treatment; original: Vol. 70, No. 1 (March 2026): "Espionage in Our AI Future" (Mulligan/RAND)	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified source-protection and institutional-control case study	28.3.2	28.3.2 source title transformed into safe curriculum treatment; original: Vol. 68, No. 2 (June 2024): OSINT in the IC	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified source-protection and institutional-control case study	28.4	28.4 source title transformed into safe curriculum treatment; original: History of SIGINT at the CIA, 1947–1970	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified source-protection and institutional-control case study	28.5	28.5 source title transformed into safe curriculum treatment; original: NSA WWII Declassified: European Axis SIGINT (9 Volumes)	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material

41.3.3.5 American Intelligence History reusable subsection contract: topic rows, artifacts, and safety duties Evidence anchor. Section 41; [266, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Declassified source-protection and institutional-control case study	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
OSS Provisional Basic Field Manual: Declassified source-protection and institutional-control case study	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Hybrid-threat indicator review using sample scenarios and policy thresholds	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
OSS Special Weapons and Devices: Declassified source-protection and institutional-control case study	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Simple Sabotage Field Manual: Declassified source-protection and institutional-control case study	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Morale Operations Field Manual: Declassified source-protection and institutional-control case study	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
CIA Cold War Operations: Declassified source-protection and institutional-control case study	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
CIA Manual of Trickery and: Declassified source-protection and institutional-control case study	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material

Lesson topic	Practice lens	Evidence artifact	Safety check
Principles of Tradecraft: Declassified source-protection and institutional-control case study	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Cognitive influence-analysis case review using sample materials	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Studies in Intelligence: Declassified source-protection and institutional-control case study	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified source-protection and institutional-control case study (28.3.1)	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified source-protection and institutional-control case study (28.3.2)	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
History of SIGINT at the: Declassified source-protection and institutional-control case study	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
NSA WWII Declassified: Declassified source-protection and institutional-control case study	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material

41.3.3.6 American Intelligence History annotated source ledger: real titles and local contribution Each source cited by this **Historical and Declassified Intelligence Services** module is paired below with its real title and a one-line note on what it contributes to **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**.

Source	Cited work	What it contributes	Status
[266, 2026]	PROV Overview	A W3C Working Group Note from 2013 that provides an overview and roadmap for the PROV family of specifications for representing and exchanging provenance information on the web. It defines provenance as information about the entities, activities, and people involved in producing data, used to assess quality, reliability, and trustworthiness.	verified source-guide
[269, 2026]	Data on the Web Best Practices	A W3C Recommendation, "Data on the Web Best Practices," published January 31, 2017 by the Data on the Web Best Practices Working Group. It offers 35 best practices for publishing and consuming data on the Web, covering metadata, licensing and provenance, data quality, dataset versioning, persistent URIs, machine-readable formats, vocabulary reuse, access methods, preservation, and feedback.	verified source-guide
[271, 2026]	DataCite Metadata Schema	The DataCite Metadata Schema page, introducing a standardized framework of core metadata properties chosen for accurate and consistent identification of research resources for citation and retrieval. It notes the latest version, 4.7 (March 2026), which adds resource types such as Poster and Presentation along with new identifier and relation-type options.	verified source-guide

Source	Cited work	What it contributes	Status
[280, 2026]	NIST SP 800-61 Rev. 3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management	NIST SP 800-61 Rev. 3, published April 2025, integrates incident response guidance into broader cybersecurity risk management aligned with the NIST Cybersecurity Framework 2.0, superseding the 2012 Rev. 2. The publication addresses cyber threat information sharing, incident handling and management practices, and procedures for detecting, responding to, and recovering from security incidents.	verified source-guide
[281, 2026]	Artificial Intelligence Cybersecurity Challenges	An ENISA (European Union Agency for Cybersecurity) report published December 15, 2020 mapping the cybersecurity challenges of artificial intelligence. It defines AI scope through a lifecycle approach, identifies the assets requiring protection within AI ecosystems, and develops a threat taxonomy classified across lifecycle stages and asset categories.	verified source-guide
[282, 2026]	AI Research: Security and Resilience	A NIST page on AI research focused on security and resilience, framing these as core characteristics of trustworthy AI under the NIST AI Risk Management Framework.	verified source-guide
[292, 2026]	Assessing Risks and Impacts of AI (ARIA): Pilot Evaluation Report	The ARIA 0.1 pilot evaluation report documents NIST's methodology for systematically assessing AI applications for risks and societal impacts, using a multi-layered evaluation approach across five participating organizations and seven submitted AI applications. The pilot employed three evaluation scenarios and three testing levels: model testing, red teaming, and field testing, supplemented by dialogue annotation, tester questionnaires, and structured measurement trees.	verified source-guide
[295, 2026]	M-25-22: Driving Efficient Acquisition of Artificial Intelligence in Government	OMB Memorandum M-25-22 (April 3, 2025), Driving Efficient Acquisition of Artificial Intelligence in Government, issued under Executive Order 13960 and related directives. It provides guidance to federal agencies for acquiring effective and trustworthy AI in a timely, cost-effective manner, and rescinds and replaces earlier memorandum M-24-18.	verified source-guide
[296, 2026]	Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile	NIST AI 600-1, the Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, a cross-sectoral companion resource to the NIST AI RMF 1.0 issued pursuant to Executive Order 14110. It identifies risks that are unique to or amplified by generative AI and organizes suggested actions for managing those risks, mapped to the AI RMF functions.	verified source-guide
[128, 2026]	Full text of "The Secret War The Office of Strategic Services in World	An Internet Archive full-text scan of the proceedings of a 1991 National Archives conference on the Office of Strategic Services (OSS), the U.S.	verified source-guide

Source	Cited work	What it contributes	Status
[129, 2026]	OSS Resources - Office of Strategic Services Society	A resource directory page from the Office of Strategic Services Society, a historical organization dedicated to preserving the record of the WWII-era OSS. The page functions as a curated library of links to external sites covering OSS history, including operations, related organizations, notable figures such as William Donovan and Allen Dulles, educational materials, and geographic theaters.	verified source-guide
[117, 2026]	Office of Strategic Services (OSS) Manuals	An article from Small Wars Journal (affiliated with Arizona State University) announcing that The Resistance Hub has compiled declassified Office of Strategic Services (OSS) manuals for public access. The OSS was the WWII predecessor to the CIA, and the documents illustrate how the United States organized clandestine activities in occupied Europe and Asia.	verified source-guide
[119, 2026]	office of strategic services - ARSOF History	See bibliography for scope.	original source-guide
[118, 2026]	Special Operations Field Manual, Strategic Services (provisional	A digitized World War II field manual from the Internet Archive, the Special Operations Field Manual, Strategic Services (provisional), issued July 18, 1944 by the U.S. Office of Strategic Services (OSS). The 32-page manual sets out the authorized functions, operational plans, methods, and organization of OSS Maritime Units and the broader Special Operations Branch.	verified source-guide
[130, 2026]	The Official CIA Manual of Trickery and Deception	A reproduction of a Cold War-era manual written by magician John Mulholland for the CIA, presented with commentary by H. Keith Melton and Robert Wallace as "The Official CIA Manual of Trickery and Deception." The book situates the manual within the history of the MKULTRA program and the long-missing magic manuals, and reproduces Mulholland's guidance on applying sleight-of-hand and misdirection techniques to covert operational tasks.	verified source-guide
[120, 2026]	PRINCIPLES TRADECRAFT	Principles of Tradecraft, a 1995 publication by Militia Free Press (a subsidiary of The Resister). The document presents an overview of intelligence and espionage concepts, with chapters covering an introduction to espionage, agents (typology, identification, recruitment, and handling), and agent organization and management including personnel and structures. It is framed as an introductory treatment rather than a comprehensive reference on intelligence requirements.	verified source-guide

Source	Cited work	What it contributes	Status
[088, 2026]	SOVIET 'ACTIVE MEASURES' FORGERY, DISINFORMATION, POLITICAL OPERATIONS	A U.S. Department of State Bureau of Public Affairs report from October 1981, released under FOIA. It catalogs Soviet 'active measures' — the Soviet term for covert influence operations — including written disinformation, control of foreign media, use of front organizations, clandestine broadcasting, blackmail, and political influence operations. Specific cases include Soviet forgeries related to the 1979 Grand Mosque seizure and NATO theater nuclear force debates.	verified source-guide
[089, 2026]	SOVIET ACTIVE MEASURES AND DISINFORMATION: OVERVIEW AND ASSESSMENT	An article by Dennis Kux published in Parameters: Journal of the US Army War College (1985) and preserved in the CIA CREST archive. It defines and distinguishes Soviet 'disinformation' and 'active measures,' situating them within a spectrum of white, gray, and black foreign influence operations. Kux examines KGB front groups, agents of influence, forgeries, and the broader strategic goal of tarnishing Western governments while advancing Soviet foreign policy.	verified source-guide
[090, 2026]	"SOVIET ACTIVE MEASURES: FORGERY, DISINFORMATION, POLITICAL OPERATIONS"	A CIA CREST record (October 1981, released March 2007) comprising a routing and record sheet from the PCS/PGLO office dated February 8, 1982, attached to the same Department of State Special Report No. 88 on Soviet active measures. The document is catalogued as an open-source CREST entry and captures the internal CIA circulation of the State Department's public report on Soviet forgery and disinformation operations.	verified source-guide
[091, 2026]	SOVIET ACTIVE MEASURES AND DISINFORMATION	A declassified-in-part 1986 CIA speech text on Soviet active measures, prepared by the Foreign Activities Branch, Third World Activities Division, Office of Soviet Analysis. It explains the KGB's use of forgeries, disinformation, and front organizations to covertly influence foreign governments and publics, illustrating with the forged 1984 Olympic KKK leaflet operation designed to discourage participation in the Los Angeles Games.	verified source-guide
[131, 2026]	Center for the Study of Intelligence - CSI	The Center for the Study of Intelligence (CSI) serves as a producer and repository of unclassified.	original source-guide
[132, 2026]	Studies in Intelligence	Studies in Intelligence is the CIA's professional journal, published by the Center for the Study of Intelligence (CSI). It covers historical, analytical, and methodological topics across the intelligence profession, and is issued quarterly in partially declassified extract form. As of 2026 the archive holds 110 issues, with the most recent being Volume 70, No. 1 (March 2026); articles are written by intelligence community professionals under their own names or pen names.	verified source-guide

Source	Cited work	What it contributes	Status
[133, 2026]	Studies in Intelligence: New Articles from The CIA's In-House Journal	This is a National Security Archive briefing book presenting declassified articles from the CIA's internal journal Studies in Intelligence, first published in 1955. The collection gathers articles obtained through Freedom of Information Act requests and litigation, spanning CIA history from the Kennedy era through the post-9/11 period.	verified source-guide
[019, 2026]	Espionage in Our AI Future: Why Human Intelligence Still Matters - CSI	By Thomas Mulligan, a researcher at the RAND Corporation who served in CIA during 2008–14.	original source-guide
[034, 2026]	Studies in Intelligence Vol. 70, No. 1 (Extracts, March 2026) - CSI	Thomas Mulligan is a researcher at the RAND Corporation and former CIA officer. Ana P.	original source-guide
[047, 2026]	How the Intelligence Community Has Held Back Open-Source	Plans and strategies for improving open-source intelligence (OSINT) operations in the Intelligence.	original source-guide
[038, 2026]	History of signals intelligence at the CIA - Open INT	A January 2018 blog post on Open INT recounting the CIA's role in signals intelligence from roughly 1947 to 1970, noting that SIGINT is often associated with the NSA but the CIA also participated. It distinguishes communications intelligence from electronic intelligence and references declassified Cold War operations including U-2 collection and a Berlin communications-tapping effort.	verified source-guide
[039, 2026]	The CIA and Signals Intelligence / National Security Archive	A 2015 briefing book from the National Security Archive, compiled by Jeffrey T. Richelson, presenting declassified documents on the CIA's signals intelligence activities from roughly 1947 to 1970. It documents the CIA's parallel SIGINT operations alongside the NSA during the Cold War, covering programs and collection efforts as well as recurring friction between the two agencies over mission overlap, budgets, and access to intelligence.	verified source-guide
[036, 2026]	European Axis Signal Intelligence in World War II	Volumes 1 - 9 of the European Axis Signal Intelligence in WWII documentation.	original source-guide
[297, 2026]	Intelligence Community Directive 203: Analytic Standards	Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products.	original source-guide

The remaining 1 cited source(s) appear in the bibliography appendix with the same verification metadata.

Where this sits. This module's overview is Section 41; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

41.3.4 American Intelligence History governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 41; [266, 2026].

41.3.5 American Intelligence History analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 28's governance-boundary section, directly verified anchors for the **Historical and Declassified Intelligence Services** lane include [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]; [Archives and Administration, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **Historical and Declassified Intelligence Services** for **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**. [266, 2026]; [269, 2026].

Curriculum topic spine: Declassified source-protection and institutional-control case study, **OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**, **OSS Provisional Basic Field Manual: Declassified source-protection and institutional-control case study**. **Verified anchor cluster:** [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]; [Archives and Administration, 2026b]; [of the Director of National Intelligence, 2026e]; [Jr., 2007]; [Agency, 2009].

Conceptual depth: turning declassified records and official histories into safe institutional lessons about analytic judgment, secrecy, oversight, technical-intelligence evolution, and reform.

Method stack: provenance review, declassification-status notation, institutional timeline building, case-to-principle translation, and uncertainty about redacted records.

Composability contract: archive source, release channel, historical context, analytic lesson, oversight implication, and modern analogy remain explicitly separated.

Known failure modes: romanticized tradecraft, presentist interpretation, redaction overclaiming, decontextualized case reuse, and translating history into operational instructions.

Defensive boundary: historical modules use declassified or public records for analysis and governance lessons only; they do not reconstruct live tactics, sources, methods, or current field procedures. Applied to **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**.

Anchor	Why it matters here
[Agency, 2026a]	Official CSI landing page for Studies in Intelligence, declassified professional reflection, analytic history, and institutional learning. Checked as of 2026-05-21; role: curriculum_anchor.
[Agency, 2026h]	Official declassified historical-release library for cryptologic history, SIGINT history, COMSEC, oral histories, and historical cases. Checked as of 2026-05-21; role: curriculum_anchor.
[Office, 2026a]	Official declassified satellite-reconnaissance program archive for CORONA, GAMBIT, POPPY, QUILL, and other historical technical-intelligence cases. Checked as of 2026-05-21; role: curriculum_anchor.
[Archives and Administration, 2026b]	Official NARA guide to CIA Record Group 263, archival provenance, record series, and declassified intelligence research pathways. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026e]	Official ODNI explanation of analytic objectivity, ombuds, and tradecraft standards. Checked as of 2026-05-21; role: curriculum_anchor.
[Jr., 2007]	Foundational analytic cognition source for bias, mental models, and structured reasoning. Checked as of 2026-06-06; role: curriculum_anchor.
[Agency, 2009]	Official structured analytic techniques primer for bias checks, alternatives, and warning analysis. Checked as of 2026-05-21; role: curriculum_anchor.

41.3.5.1 American Intelligence History evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **Historical and Declassified Intelligence Services** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [266, 2026]; [269, 2026].

41.3.6 American Intelligence History agentic boundary: assist, approve, block, and record

Evidence anchor. Section 41; [266, 2026].

AGEINT translation is bounded by the **Historical and Declassified Intelligence Services** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**.

41.3.6.1 American Intelligence History permitted defensive utility: curriculum uses and safe outputs

Evidence anchor. Section 41; [266, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**.

41.3.6.2 American Intelligence History excluded operational boundary: blocked actions and stop rules

Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [266, 2026]; [269, 2026] and **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

41.3.7 American Intelligence History governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 41; [266, 2026].

Governance is practiced as a gate on the **Historical and Declassified Intelligence Services** lane. Learners use the **Historical Case-Translation Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted

artifact must stop for human review while using **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**.

41.3.7.1 American Intelligence History governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [266, 2026]; [269, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Historical and Declassified Intelligence Services** failure modes and the **Historical Case-Translation Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

41.3.7.2 American Intelligence History evidence package handoff: appendices, records, and reuse

Evidence anchor. Section 41; [266, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Historical Case-Translation Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**.

41.3.7.3 American Intelligence History current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**. [266, 2026]; [269, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_cia_center_for_study_of_intelligence` for **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**?	Center for the Study of Intelligence; lane `historical_declassified_sources`; checked 2026-05-21.	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary; Official CSI landing page for Studies in Intelligence, declassified professional reflection, analytic history, and institutional learning.
What does the module inherit from `official_nsa_historical_releases` for **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**?	NSA Historical Releases; lane `historical_declassified_sources`; checked 2026-05-21.	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary; Official declassified historical-release library for cryptologic history, SIGINT history, COMSEC, oral histories, and historical cases.
What does the module inherit from `official_nro_declassified_programs` for **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**?	Declassified NRO Programs and Projects; lane `historical_declassified_sources`; checked 2026-05-21.	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary; Official declassified satellite-reconnaissance program archive for CORONA, GAMBIT, POPPY, QUILL, and other historical technical-intelligence cases.
What does the module inherit from `official_nara_cia_records` for **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**?	Records of the Central Intelligence Agency; lane `historical_declassified_sources`; checked 2026-05-21.	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary; Official NARA guide to CIA Record Group 263, archival provenance, record series, and declassified intelligence research pathways.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 41; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

41.3.8 American Intelligence History assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 41; [266, 2026].

41.3.9 American Intelligence History assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 41; [266, 2026].

41.3.9.1 American Intelligence History capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study** and [266, 2026]; [269, 2026].

41.3.9.2 American Intelligence History instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study** and [266, 2026]; [269, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

41.3.9.3 American Intelligence History assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Declassified source-protection and institutional-control case study	Completed **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study	Completed **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
OSS Provisional Basic Field Manual: Declassified source-protection and institutional-control case study	Completed **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

41.3.10 American Intelligence History refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [266, 2026]; [269, 2026] and **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**.

41.3.10.1 American Intelligence History refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**. The local signals begin with [266, 2026]; [269, 2026].

41.3.10.2 American Intelligence History claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**, and the source spine for these checks begins with [266, 2026]; [269, 2026].

41.3.11 American Intelligence History reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [266, 2026]; [269, 2026].

Triangulation anchors. In module 28's review-checklist section, directly verified anchors for the **Historical and Declassified Intelligence Services** lane include [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]; [Archives and Administration, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study**. [266, 2026]; [269, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.

- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

41.3.12 American Intelligence History learning-path links: module map, overview, and curriculum atlas

These links keep **Declassified source-protection and institutional-control case study; OSS Secret Intelligence Manual: Declassified source-protection and institutional-control case study** paired with the orientation atlas, the parent unit, and the previous and next modules, so a reader can trace which claims and caveats are inherited rather than re-derived here. Anchored at [266, 2026]; [269, 2026].
Section 2, Section 39, Section 40, Section 42

42 British and Allied Intelligence

42.0.1 British and Allied Intelligence figures and course links: visual evidence, source flow, and navigation

The module uses Figure 83 and Figure 79 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.

Navigation links: Section 2, Section 39, Section 41, Section 43.

This module teaches the **Historical and Declassified Intelligence Services** lane through a bounded, source-backed coursebook chapter. [266, 2026]; [269, 2026].

42.1 Historical and Declassified Intelligence Services frame for British and Allied Intelligence: source context, topic focus, and reader task

Evidence anchor. Section 42; [266, 2026].

42.1.1 British and Allied Intelligence orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 42; [266, 2026].

42.1.2 British and Allied Intelligence conceptual primer: source context, core model, and reader task

This chapter teaches historical intelligence study as declassified evidence review: archives teach institutional lessons when provenance, redaction, context, and modern boundaries are explicit. The chapter uses **Historical Case-Translation Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**.

The central distinction is to separate historical lesson from reconstruction of live tactics or current sources and methods. Core topics include **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds; GCHQ and the BRUSA/UKUSA Agreements**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.

Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [266, 2026]; [269, 2026].

Learners move from vocabulary and the **Historical Case-Translation Lens** distinction through topic lessons on **Declassified source-protection and institutional-control case study** with evidence and misconception checks, then assemble a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** with safety and rights gates.

42.1.3 British and Allied Intelligence learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 42; [266, 2026].

- Connect **Declassified source-protection and institutional-control case study and Hybrid-threat indicator review using sample scenarios and policy thresholds** to **Historical and Declassified Intelligence Services** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate historical lesson from reconstruction of live tactics or current sources and methods; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as romanticized tradecraft, presentist interpretation, redaction overclaiming, decontextualized case reuse, and translating history into operational instructions, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: historical modules use declassified or public records for analysis and governance lessons only; they do not reconstruct live tactics, sources, methods, or current field procedures.

42.1.4 British and Allied Intelligence core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 42; [266, 2026].

Term	Working definition
Declassification context	the release channel, date, and limits of an official historical source
Redaction caveat	the warning that missing text may change interpretation
Institutional lesson	the durable governance or analytic principle drawn from a case
Presentism	the error of forcing modern assumptions onto a historical record
Modern analogy	a bounded comparison that preserves differences between eras
Oversight failure	a documented breakdown in review, records, or accountability visible in the archive
Source-protection lesson	the historical principle about protecting people and methods without reconstructing live tradecraft
Declassified source-protection and…	Key terms: Declassified, protection, institutional.
Hybrid-threat indicator review using sample…	Key terms: Hybrid, threat, indicator.

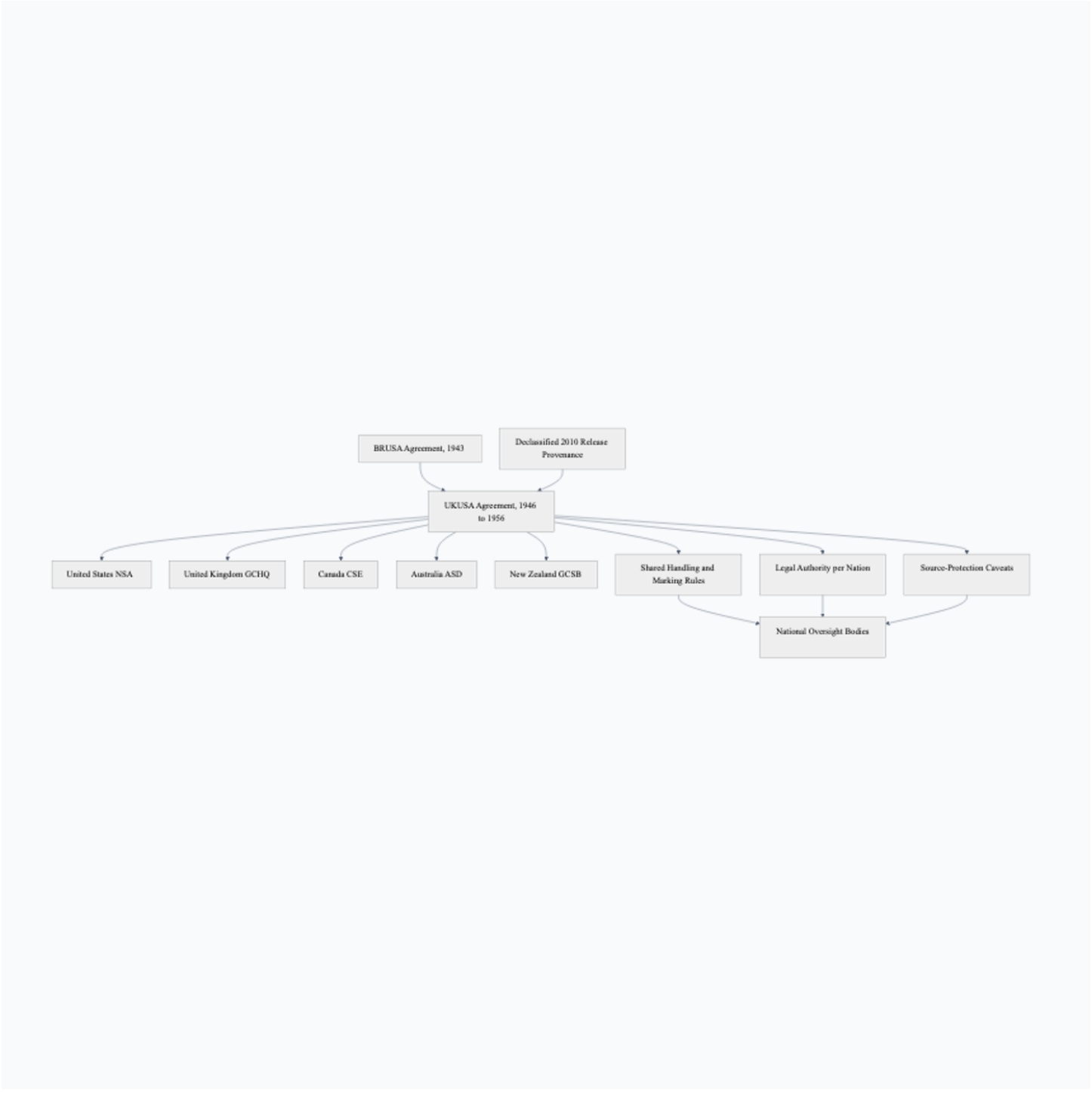


Figure 83: A governance map of the postwar UKUSA signals-intelligence framework showing the Five Eyes partners, the agreements that bind them, and the shared handling and oversight rules. In the historical intelligence services / british and allied intelligence section, it lets readers compare BRUSA Agreement, 1943, UKUSA Agreement, 1946 to 1956, United States NSA, and United Kingdom GCHQ so the visual functions as a traceable course aid rather than an unscoped assertion.

42.2 Historical Case-Translation Lens path for British and Allied Intelligence: lesson cluster, safe artifact, and review

Evidence anchor. Section 42; [266, 2026].

42.2.1 British and Allied Intelligence practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 42; [266, 2026].

42.2.2 British and Allied Intelligence topic lessons: source-backed concepts and transfer tasks

This module builds historical intelligence study as declassified evidence review: archives teach institutional lessons when provenance, redaction, context, and modern boundaries are explicit. The sequence opens with **Declassified source-protection and institutional-control case study**, **Hybrid-threat indicator review using sample scenarios and policy thresholds**, **GCHQ and the BRUSA/UKUSA Agreements** and applies the **Historical Case-Translation Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 79; module overview Section 42; curriculum atlas Section 2.

Triangulation anchors. In module 29's topic-lessons section, directly verified anchors for the **Historical and Declassified Intelligence Services** lane include [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]; [Archives and Administration, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

42.2.2.1 Lesson 1: Declassified source-protection and institutional-control case study

Concept. Declassified source-protection and institutional-control case study studies the declassified record for institutional lessons about oversight, source protection, and limits on translating history into practice.

Why it matters. Declassified source-protection connects classroom vocabulary to Historical and Declassified Intelligence Services practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Declassified source-protection and institutional-control case study rests on [007, 2026]. The lead source's own note reads: It is SIS's task to pursue policy objectives by unorthodox means and to amass useful information. Use it for the working definition that **Declassified source-protection and institutional-control case study** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. For **Declassified source-protection**, reason from the sources cited in this row. [007, 2026] It is SIS's task to pursue policy objectives by unorthodox means and to amass useful information. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Declassified source-protection**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **Declassified source-protection and institutional-control case**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape **Declassified source-protection** work as a **declassified case-to-principle card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Transfer **Declassified source-protection** from this module to a second motif by preserving declassified-source interpretation and case-to-principle translation, replacing action with audit, and naming the blocked use.

42.2.2.2 Lesson 2: Hybrid-threat indicator review using sample scenarios and policy thresholds

Concept. Hybrid-threat indicator review using sample scenarios and policy thresholds reads special-operations intelligence as support to accountable planning with explicit authority and oversight fields.

Why it matters. Without explicit treatment of **Hybrid-threat indicator review**, romanticized tradecraft undermines declassified-source interpretation and case-to-principle translation review; the lesson builds the habit to separate historical lesson from reconstruction of live tactics or current sources and methods.

Source support. Hybrid-threat indicator review using sample scenarios and policy thresholds rests on [134, 2026]. The closest source to this row notes: How To Be A Spy: The WW2 SOE Training Manual - Denis Rigden · The CIA Guide to Clandestine. Use it for pinning down the scope of **Hybrid-threat indicator review using sample scenarios and policy thresholds**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. For **Hybrid-threat indicator review**, work from the cited evidence behind this row. [134, 2026] How To Be A Spy: The WW2 SOE Training Manual - Denis Rigden · The CIA Guide to Clandestine. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Hybrid-threat indicator review**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must name the indicator descriptor, the bounded claim about **Hybrid-threat indicator review using sample**, the attribution caveat, the threshold uncertainty, the non-attribution boundary, and the reviewer who approves the policy read. Shape **Hybrid-threat indicator review** work as a **declassified case-to-principle card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Hybrid-threat indicator review**: that activity falling below an obvious threshold is therefore ungoverned, rather than still bound by escalation limits and accountable review.

Transfer task. Apply this module's safe boundary for **Hybrid-threat indicator review** to another artifact while keeping declassified-source interpretation and case-to-principle translation and reviewer ownership explicit.

42.2.2.3 Lesson 3: GCHQ and the BRUSA/UKUSA Agreements

Concept. GCHQ and the BRUSA/UKUSA Agreements uses the sharing arrangement to distinguish alliance governance, handling rules, legal authority, and source caveats.

Why it matters. GCHQ and the BRUSA/UKUSA Agreements matters in the **Historical and Declassified Intelligence Services** lane because declassified-source interpretation and case-to-principle translation evidence must stay separate from judgment; romanticized tradecraft is a common failure.

Source support. GCHQ and the BRUSA/UKUSA Agreements rests on [011, 2026] and [135, 2026]. The most specific cited work observes: It traces the 1946 BRUSA agreement on intelligence exchange, Canada's negotiation toward equal partnership in 1949, and the gradual integration of Australia and New Zealand through the 1950s. Use them for pinning down the scope of **GCHQ and the BRUSA/UKUSA Agreements**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. For **GCHQ and the BRUSA/UKUSA Agreements**, reason from the sources cited in this row. [011, 2026] A curated collection from Unredacted UK presenting documents declassified by the NSA and GCHQ in 2010 relating to US-UK signals intelligence cooperation. It covers the 1946 British-US Communications Agreement (BRUSA), its wartime origins from 1940, and its evolution into the 1956 UKUSA Agreement and the broader Five Eyes alliance. [135, 2026] A briefing from Unredacted, a UK investigative outlet, covering the early development of the UKUSA

Agreement, the postwar US-UK signals-intelligence framework that became the basis for the Five Eyes alliance. It traces the 1946 BRUSA agreement on intelligence exchange, Canada's negotiation toward equal partnership in 1949, and the gradual integration of Australia and New Zealand through the 1950s. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. Build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must name the source descriptor, the bounded claim about **GCHQ and the BRUSA/UKUSA Agreements**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape this subject work as a **declassified case-to-principle card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that GCHQ and the BRUSA/UKUSA Agreements is optional whenever separate historical lesson from reconstruction of live tactics or current sources and methods feels inconvenient.

Transfer task. Transfer **GCHQ and the BRUSA/UKUSA Agreements** to a second module by preserving declassified-source interpretation and case-to-principle translation, changing the source evidence, and naming a new reviewer.

42.2.2.4 Lesson 4: Five Eyes Archive: Key Declassified Documents

Concept. Five Eyes Archive: Key Declassified Documents uses the sharing arrangement to distinguish alliance governance, handling rules, legal authority, and source caveats.

Why it matters. Five Eyes Archive connects classroom vocabulary to Historical and Declassified Intelligence Services practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Five Eyes Archive: Key Declassified Documents rests on [010, 2026], [041, 2026], and [042, 2026]. The closest source to this row notes: The collection traces the emergence and evolution of bilateral and multilateral agreements from the postwar era, including the BRUSA and UKUSA agreements, drawing on records from UK, US, and Australian agencies plus freedom-of-information releases. Use them for pinning down the scope of **Five Eyes Archive: Key Declassified Documents**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. Read **Five Eyes Archive** against the works cited for this row. [010, 2026] An online archive maintained by Unredacted UK that compiles declassified government documents on intelligence sharing among the Five Eyes nations (United States, United Kingdom, Canada, Australia, and New Zealand). The collection traces the emergence and evolution of bilateral and multilateral agreements from the postwar era, including the BRUSA and UKUSA agreements, drawing on records from UK, US, and Australian agencies plus freedom-of-information releases. [041, 2026] A collection page from Unredacted, a UK-based organization focused on declassified government records. It assembles over 70 documents obtained through a 2017 Freedom of Information Act legal challenge led by Privacy International, drawn from US agencies including the NSA, State Department, and Department of Defense. [042, 2026] A briefing from Unredacted examining previously classified Five Eyes documents released to Privacy International following a 2017 US freedom of information request. The materials, spanning 1945 to 2016, trace the development and functioning of the UKUSA Agreement underpinning intelligence cooperation among the US, UK, Canada, Australia, and New Zealand. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Five Eyes Archive**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must name the source descriptor, the bounded claim about **Five Eyes Archive**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Five Eyes Archive** work as a **declassified case-to-principle card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that Five Eyes Archive: Key Declassified Documents establishes intent without reviewing alternative explanations.

Transfer task. Transfer **Five Eyes Archive** to a second module by preserving declassified-source interpretation and case-to-principle translation, changing the source evidence, and naming a new reviewer.

42.2.3 British and Allied Intelligence worked safe example: synthetic inputs, evidence, and review

Worked example: a sample seminar studies a declassified reform episode and extracts an oversight lesson without reconstructing current sources and methods. [266, 2026]; [269, 2026].

Triangulation anchors. In module 29's worked-example section, directly verified anchors for the **Historical and Declassified Intelligence Services** lane include [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]; [Archives and Administration, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **declassified-source interpretation**. Learners use a **declassified case-to-principle card** and keep this boundary visible: No current sources-and-methods reconstruction, operational emulation, or tactical transfer.

Frame. The classroom question centers on **Declassified source-protection and institutional-control case study**. Excluded actions stay explicit, and the **Historical Case-Translation Lens** planning question is: Which declassified source, release context, institutional lesson, and modern boundary can be carried forward without recreating operations?

Inputs. For the **Declassified source-protection and institutional-control case study** scenario, use public archive metadata, a short excerpt, a timeline template, and an oversight-question worksheet. The Historical Case-Translation Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Declassified source-protection and institutional-control case study**, students record provenance, mark redactions, build timeline, distinguish known from unknown, and extract a governance lesson. Pause whenever an inference about Declassified source-protection and institutional-control case study appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Declassified source-protection and institutional-control case study** classroom scenario; unit artifact = declassified case-to-principle card; evidence = allowed inputs; method = declassified-source interpretation and case-to-principle translation; output = a historical case card with release context, caveats, lesson, and evidence-bounded boundary; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Declassified source-protection and institutional-control case study** as "Historical Case-Translation Lens confirms it" is not enough. The revision ties the claim to declassified-source interpretation and case-to-principle translation, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Declassified source-protection and institutional-control case study** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

42.2.4 British and Allied Intelligence practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Historical Case-Translation Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**.

Triangulation anchors. In module 29's practice-sequence section, directly verified anchors for the **Historical and Declassified Intelligence Services** lane include [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]; [Archives and Administration, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Declassified source-protection and institutional-control case study, Hybrid-threat indicator review using sample scenarios and policy thresholds, GCHQ and the BRUSA/UKUSA Agreements; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Historical and Declassified Intelligence Services** lane.
2. Frame	Answer the lens question: Which declassified source, release context, institutional lesson, and modern boundary can be carried forward without recreating operations?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Declassified source-protection and institutional-control case study: historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the declassified case-to-principle card fields for Declassified source-protection and institutional-control case study.	Unit profile note.	Evidence artifacts include release metadata, redaction caveat.
4. Challenge	Test the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.	Failure-mode note.	The artifact applies the key distinction: separate historical lesson from reconstruction of live tactics or current sources and methods.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

42.2.4.1 British and Allied Intelligence instructor notes: source reasoning, review points, and studio focus Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**. [266, 2026]; [269, 2026].

42.2.4.2 British and Allied Intelligence extension exercise: peer validation and refresh trigger review **Evidence anchor.** Section 42; [266, 2026].

Have learners swap artifacts and apply the **Historical Case-Translation Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**.

42.2.5 British and Allied Intelligence knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 42; [266, 2026].

1. Explain how **Declassified source-protection and institutional-control case study** is defined here; name the source descriptor that supports the definition.
2. Contrast **Declassified source-protection and institutional-control case study** with **Hybrid-threat indicator review using sample scenarios and policy thresholds** using the **Historical Case-Translation Lens** artifact fields.
3. Identify one failure mode from the **Historical and Declassified Intelligence Services** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which institutional lesson is defensible from the record, and which claim reconstructs live tradecraft?
5. Correct this misconception: that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

42.2.5.1 British and Allied Intelligence answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Declassified source-protection and institutional-control case study** without source evidence, uncertainty, or a safe transfer task.

42.3 British and Allied Intelligence assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 42; [266, 2026].

42.3.1 British and Allied Intelligence evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 42; [266, 2026].

42.3.2 British and Allied Intelligence transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 42; [266, 2026].

42.3.2.1 British and Allied Intelligence lineage and source tradition: profile, concepts, and first anchors This sits in the **Historical and Declassified Intelligence Services** lineage: turning declassified records and official histories into safe institutional lessons about analytic judgment, secrecy, oversight, technical-intelligence evolution, and reform. [266, 2026]; [269, 2026].

42.3.2.2 British and Allied Intelligence working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 42; [266, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**, with provenance and reviewability throughout.

42.3.2.3 British and Allied Intelligence knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [266, 2026]; [269, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

42.3.2.4 British and Allied Intelligence transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 42; [266, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**.
- **Evidence contract:** keep the **Historical and Declassified Intelligence Services** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

42.3.2.5 British and Allied Intelligence profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 42; [266, 2026].

The matched profile emphasizes turning declassified records and official histories into safe institutional lessons about analytic judgment, secrecy, oversight, technical-intelligence evolution, and reform. The method stack is provenance review, declassification-status notation, institutional timeline building, case-to-principle translation, and uncertainty about redacted records; the local topic cluster is **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**.

42.3.3 British and Allied Intelligence evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 42; [266, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Historical and Declassified Intelligence Services** profile tells reviewers what evidence is strong enough for the module artifact built around **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**.

42.3.3.1 British and Allied Intelligence guide source spine: inherited keys and local citation roles Primary guide citations: [266, 2026]; [269, 2026]; [270, 2026]; [273, 2026]; [276, 2026]; [285, 2026]; [286, 2026]; [290, 2026]; [294, 2026]; [007, 2026]; [134, 2026]; [011, 2026]; [135, 2026]; [010, 2026]; [041, 2026]; [042, 2026].

42.3.3.2 British and Allied Intelligence verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [266, 2026]; [269, 2026].

Tier	What counts	How it is used
Source guide	[266, 2026]; [269, 2026]; [270, 2026]; [273, 2026]; [276, 2026]; [285, 2026]; [286, 2026]; [290, 2026]; [294, 2026]; [007, 2026]; [134, 2026]; [011, 2026]; [135, 2026]; [010, 2026]; [041, 2026]; [042, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 29's source-canon section, directly verified anchors for the **Historical and Declassified Intelligence Services** lane include [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]; [Archives and Administration, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds** and [266, 2026]; [269, 2026], but only directly verified source URLs are encoded as citations.

42.3.3.3 British and Allied Intelligence intelligence practice lens: evidence artifact and safety check Practice lens: **Historical Case-Translation Lens** for **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**. [266, 2026]; [269, 2026].

Planning question: Which declassified source, release context, institutional lesson, and modern boundary can be carried forward without recreating operations?

Evidence artifact: historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary.

Validation rule: distinguish what the record shows, what remains redacted or unknown, and which governance lesson is defensibly transferable. Applied to **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**.

Handoff contract: handoff preserves archive citation, historical context, analytic lesson, oversight implication, and modern analogy as separate fields.

Safety check: exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material.

42.3.3.4 British and Allied Intelligence runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 42; [266, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	29.99	29.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind British and Allied Intelligence to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Bounded autonomy, procurement, incident-response, and assurance studio	29.101	29.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for British and Allied Intelligence	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Model-card, recoverability, retention, and learner-support evidence package	29.102	29.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for British and Allied Intelligence	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified source-protection and institutional-control case study	29.1	29.1 source title transformed into safe curriculum treatment; original: MI6/SIS: Structure and Cold War Tradecraft	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Hybrid-threat indicator review using sample scenarios and policy thresholds	29.2	29.2 source title transformed into safe curriculum treatment; original: SOE: Special Operations Executive Training (WWII)	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
GCHQ and the BRUSA/UKUSA Agreements	29.3	29.3 GCHQ and the BRUSA/UKUSA Agreements	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Five Eyes Archive: Key Declassified Documents	29.4	29.4 Five Eyes Archive: Key Declassified Documents	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material

42.3.3.5 British and Allied Intelligence reusable subsection contract: topic rows, artifacts, and safety duties **Evidence anchor.** Section 42; [266, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Declassified source-protection and institutional-control case study	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Hybrid-threat indicator review using sample scenarios and policy thresholds	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
GCHQ and the BRUSA/UKUSA Agreements	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Five Eyes Archive: Key Declassified Documents	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material

42.3.3.6 British and Allied Intelligence annotated source ledger: real titles and local contribution Each source cited by this **Historical and Declassified Intelligence Services** module is paired below with its real title and a one-line note on what it contributes to **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**.

Source	Cited work	What it contributes	Status
[266, 2026]	PROV Overview	A W3C Working Group Note from 2013 that provides an overview and roadmap for the PROV family of specifications for representing and exchanging provenance information on the web. It defines provenance as information about the entities, activities, and people involved in producing data, used to assess quality, reliability, and trustworthiness.	verified source-guide
[269, 2026]	Data on the Web Best Practices	A W3C Recommendation, "Data on the Web Best Practices," published January 31, 2017 by the Data on the Web Best Practices Working Group. It offers 35 best practices for publishing and consuming data on the Web, covering metadata, licensing and provenance, data quality, dataset versioning, persistent URIs, machine-readable formats, vocabulary reuse, access methods, preservation, and feedback.	verified source-guide

Source	Cited work	What it contributes	Status
[270, 2026]	NIST Big Data Interoperability Framework	NIST Special Publication 1500-1 (revised edition by Chang and Grady) establishes foundational terminology and consensus definitions for Big Data through the NIST Big Data Public Working Group. The volume defines Big Data characteristics, taxonomy, and a reference architecture assigning roles to Application Providers, Data Consumers, Data Providers, and System Orchestrators.	verified source-guide
[273, 2026]	WCAG 2 Overview	The W3C Web Accessibility Initiative overview of the Web Content Accessibility Guidelines (WCAG), an international standard for making web content accessible to people with disabilities. It explains that WCAG is organized around four principles (perceivable, operable, understandable, robust) with testable success criteria at three conformance levels (A, AA, AAA), and covers versions 2.0, 2.1, and 2.2.	verified source-guide
[276, 2026]	What is a Data Protection Impact Assessment and When Is This Mandatory?	A European Data Protection Board FAQ page, part of its data protection guide for small businesses, explaining Data Protection Impact Assessments (DPIAs) and when they are mandatory. It describes a DPIA as a written assessment of the impact of a planned processing operation, required when processing poses high risks to individuals' rights.	verified source-guide
[285, 2026]	NIST AI Resource Center	The NIST AI Resource Center (AIRC), a government platform supporting implementation of the NIST AI Risk Management Framework, a voluntary framework for managing AI risk. It provides the core framework along with a playbook of practical actions, profiles tailored to specific sectors and technologies, use cases, and crosswalks linking the framework to other governance structures.	verified source-guide
[286, 2026]	Model Cards for Model Reporting	The arXiv abstract for "Model Cards for Model Reporting" (2018) by Mitchell, Wu, Zaldivar, and colleagues, which introduces a framework for transparent documentation of machine learning models. Model cards are short accompanying documents that report a model's benchmarked performance across varied conditions, including different cultural, demographic, and phenotypic groups, along with intended use, evaluation methodology, and deployment considerations.	verified source-guide
[290, 2026]	NIST SP 800-218A: Secure Software Development Practices for Generative AI and Dual-Use Foundation Models	NIST Special Publication 800-218A (July 2024), which augments the Secure Software Development Framework with practices specific to AI model development across the software lifecycle. Produced in response to Executive Order 14110, it addresses AI model producers, developers building on those models, and acquirers of AI systems, and is designed to be used alongside NIST SP 800-218.	verified source-guide

Source	Cited work	What it contributes	Status
[294, 2026]	M-25-21: Accelerating Federal Use of AI through Innovation, Governance, and Public Trust	An April 2025 Office of Management and Budget memorandum (M-25-21) directing executive branch agencies on federal use of artificial intelligence. Issued under Executive Order 14179, it instructs agencies to accelerate adoption of AI to improve public services and government efficiency while maintaining safeguards for civil rights, civil liberties, and privacy.	verified source-guide
[007, 2026]	THE FRIENDS BRITAIN'S POST-WAR SECRET INTELLIGENCE	It is SIS's task to pursue policy objectives by unorthodox means and to amass useful information.	original source-guide
[134, 2026]	What is your reading list for (counter)intelligence/tradecraft?	How To Be A Spy: The WW2 SOE Training Manual - Denis Rigden · The CIA Guide to Clandestine.	original source-guide
[011, 2026]	BRUSA and UKUSA Agreements: GCHQ and NSA	A curated collection from Unredacted UK presenting documents declassified by the NSA and GCHQ in 2010 relating to US-UK signals intelligence cooperation. It covers the 1946 British-US Communications Agreement (BRUSA), its wartime origins from 1940, and its evolution into the 1956 UKUSA Agreement and the broader Five Eyes alliance.	verified source-guide
[135, 2026]	The origins of the UKUSA Agreement	A briefing from Unredacted, a UK investigative outlet, covering the early development of the UKUSA Agreement, the postwar US-UK signals-intelligence framework that became the basis for the Five Eyes alliance. It traces the 1946 BRUSA agreement on intelligence exchange, Canada's negotiation toward equal partnership in 1949, and the gradual integration of Australia and New Zealand through the 1950s.	verified source-guide
[010, 2026]	The Five Eyes Archive	An online archive maintained by Unredacted UK that compiles declassified government documents on intelligence sharing among the Five Eyes nations (United States, United Kingdom, Canada, Australia, and New Zealand). The collection traces the emergence and evolution of bilateral and multilateral agreements from the postwar era, including the BRUSA and UKUSA agreements, drawing on records from UK, US, and Australian agencies plus freedom-of-information releases.	verified source-guide
[041, 2026]	Five Eyes FOIA disclosures	A collection page from Unredacted, a UK-based organization focused on declassified government records. It assembles over 70 documents obtained through a 2017 Freedom of Information Act legal challenge led by Privacy International, drawn from US agencies including the NSA, State Department, and Department of Defense.	verified source-guide

Source	Cited work	What it contributes	Status
[042, 2026]	Five Eyes FOIA disclosures: key documents	A briefing from Unredacted examining previously classified Five Eyes documents released to Privacy International following a 2017 US freedom of information request. The materials, spanning 1945 to 2016, trace the development and functioning of the UKUSA Agreement underpinning intelligence cooperation among the US, UK, Canada, Australia, and New Zealand.	verified source-guide

Where this sits. This module's overview is Section 42; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

42.3.4 British and Allied Intelligence governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 42; [266, 2026].

42.3.5 British and Allied Intelligence analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 29's governance-boundary section, directly verified anchors for the **Historical and Declassified Intelligence Services** lane include [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]; [Archives and Administration, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Research lane: **Historical and Declassified Intelligence Services** for **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**. [266, 2026]; [269, 2026].
Curriculum topic spine: Declassified source-protection and institutional-control case study, **Hybrid-threat indicator review using sample scenarios and policy thresholds**, **GCHQ and the BRUSA/UKUSA Agreements**. **Verified anchor cluster:** [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]; [Archives and Administration, 2026b]; [of the Director of National Intelligence, 2026e]; [Jr., 2007]; [Agency, 2009].
Conceptual depth: turning declassified records and official histories into safe institutional lessons about analytic judgment, secrecy, oversight, technical-intelligence evolution, and reform.
Method stack: provenance review, declassification-status notation, institutional timeline building, case-to-principle translation, and uncertainty about redacted records.
Composability contract: archive source, release channel, historical context, analytic lesson, oversight implication, and modern analogy remain explicitly separated.
Known failure modes: romanticized tradecraft, presentist interpretation, redaction overclaiming, decontextualized case reuse, and translating history into operational instructions.
Defensive boundary: historical modules use declassified or public records for analysis and governance lessons only; they do not reconstruct live tactics, sources, methods, or current field procedures. Applied to **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**.

Anchor	Why it matters here
[Agency, 2026a]	Official CSI landing page for Studies in Intelligence, declassified professional reflection, analytic history, and institutional learning. Checked as of 2026-05-21; role: curriculum_anchor.
[Agency, 2026h]	Official declassified historical-release library for cryptologic history, SIGINT history, COMSEC, oral histories, and historical cases. Checked as of 2026-05-21; role: curriculum_anchor.
[Office, 2026a]	Official declassified satellite-reconnaissance program archive for CORONA, GAMBIT, POPPY, QUILL, and other historical technical-intelligence cases. Checked as of 2026-05-21; role: curriculum_anchor.
[Archives and Administration, 2026b]	Official NARA guide to CIA Record Group 263, archival provenance, record series, and declassified intelligence research pathways. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026e]	Official ODNI explanation of analytic objectivity, ombuds, and tradecraft standards. Checked as of 2026-05-21; role: curriculum_anchor.
[Jr., 2007]	Foundational analytic cognition source for bias, mental models, and structured reasoning. Checked as of 2026-06-06; role: curriculum_anchor.
[Agency, 2009]	Official structured analytic techniques primer for bias checks, alternatives, and warning analysis. Checked as of 2026-05-21; role: curriculum_anchor.

42.3.5.1 British and Allied Intelligence evidence standard and citation floor: source families and discovery limits Official guidance supplies governance, safety, and legal constraints for the **Historical and Declassified Intelligence Services** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [266, 2026]; [269, 2026].

42.3.6 British and Allied Intelligence agentic boundary: assist, approve, block, and record

Evidence anchor. Section 42; [266, 2026].
AGEINT translation is bounded by the **Historical and Declassified Intelligence Services** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**.

42.3.6.1 British and Allied Intelligence permitted defensive utility: curriculum uses and safe outputs **Evidence anchor.** Section 42; [266, 2026].
The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**.

42.3.6.2 British and Allied Intelligence excluded operational boundary: blocked actions and stop rules Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [266, 2026]; [269, 2026] and **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

42.3.7 British and Allied Intelligence governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 42; [266, 2026].
Governance is practiced as a gate on the **Historical and Declassified Intelligence Services** lane. Learners use the **Historical Case-Translation Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact

must stop for human review while using **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**.

42.3.7.1 British and Allied Intelligence governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [266, 2026]; [269, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Historical and Declassified Intelligence Services** failure modes and the **Historical Case-Translation Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

42.3.7.2 British and Allied Intelligence evidence package handoff: appendices, records, and reuse

Evidence anchor. Section 42; [266, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Historical Case-Translation Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**.

42.3.7.3 British and Allied Intelligence current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**. [266, 2026]; [269, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_cia_center_for_study_of_intelligence` for **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**?	Center for the Study of Intelligence; lane `historical_declassified_sources`; checked 2026-05-21.	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary; Official CSI landing page for Studies in Intelligence, declassified professional reflection, analytic history, and institutional learning.
What does the module inherit from `official_nsa_historical_releases` for **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**?	NSA Historical Releases; lane `historical_declassified_sources`; checked 2026-05-21.	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary; Official declassified historical-release library for cryptologic history, SIGINT history, COMSEC, oral histories, and historical cases.
What does the module inherit from `official_nro_declassified_programs` for **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**?	Declassified NRO Programs and Projects; lane `historical_declassified_sources`; checked 2026-05-21.	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary; Official declassified satellite-reconnaissance program archive for CORONA, GAMBIT, POPPY, QUILL, and other historical technical-intelligence cases.
What does the module inherit from `official_nara_cia_records` for **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**?	Records of the Central Intelligence Agency; lane `historical_declassified_sources`; checked 2026-05-21.	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary; Official NARA guide to CIA Record Group 263, archival provenance, record series, and declassified intelligence research pathways.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 42; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

42.3.8 British and Allied Intelligence assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 42; [266, 2026].

42.3.9 British and Allied Intelligence assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 42; [266, 2026].

42.3.9.1 British and Allied Intelligence capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds** and [266, 2026]; [269, 2026].

42.3.9.2 British and Allied Intelligence instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds** and [266, 2026]; [269, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

42.3.9.3 British and Allied Intelligence assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Declassified source-protection and institutional-control case study	Completed **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Hybrid-threat indicator review using sample scenarios and policy thresholds	Completed **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
GCHQ and the BRUSA/UKUSA Agreements	Completed **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

42.3.10 British and Allied Intelligence refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [266, 2026]; [269, 2026] and **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**.

42.3.10.1 British and Allied Intelligence refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**. The local signals begin with [266, 2026]; [269, 2026].

42.3.10.2 British and Allied Intelligence claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**, and the source spine for these checks begins with [266, 2026]; [269, 2026].

42.3.11 British and Allied Intelligence reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [266, 2026]; [269, 2026].

Triangulation anchors. In module 29's review-checklist section, directly verified anchors for the **Historical and Declassified Intelligence Services** lane include [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]; [Archives and Administration, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds**. [266, 2026]; [269, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.

- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

42.3.12 British and Allied Intelligence learning-path links: module map, overview, and curriculum atlas

These links keep **Declassified source-protection and institutional-control case study; Hybrid-threat indicator review using sample scenarios and policy thresholds** paired with the orientation atlas, the parent unit, and the previous and next modules, so a reader can trace which claims and caveats are inherited rather than re-derived here. Anchored at [266, 2026]; [269, 2026].

Section 2, Section 39, Section 41, Section 43

43 Israeli and Continental Services

43.0.1 Israeli and Continental Services figures and course links: visual evidence, source flow, and navigation

The module uses Figure 84 and Figure 79 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 39, Section 42, Section 44.
This module teaches the **Historical and Declassified Intelligence Services** lane through a bounded, source-backed coursebook chapter. [266, 2026]; [267, 2026].

43.1 Historical and Declassified Intelligence Services frame for Israeli and Continental Services: source context, topic focus, and reader task

Evidence anchor. Section 43; [266, 2026].

43.1.1 Israeli and Continental Services orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 43; [266, 2026].

43.1.2 Israeli and Continental Services conceptual primer: source context, core model, and reader task

This chapter teaches historical intelligence study as declassified evidence review: archives teach institutional lessons when provenance, redaction, context, and modern boundaries are explicit. The chapter uses **Historical Case-Translation Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**.
The central distinction is to separate historical lesson from reconstruction of live tactics or current sources and methods. Core topics include **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case; Declassified covert-action oversight and source-protection case**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [266, 2026]; [267, 2026].
Learners move from vocabulary and the **Historical Case-Translation Lens** distinction through topic lessons on **Declassified source-protection and institutional-control case study** with evidence and misconception checks, then assemble a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** with safety and rights gates.

43.1.3 Israeli and Continental Services learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 43; [266, 2026].

- Connect **Declassified source-protection and institutional-control case study and Declassified cover-identity and source-protection case** to **Historical and Declassified Intelligence Services** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate historical lesson from reconstruction of live tactics or current sources and methods; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as romanticized tradecraft, presentist interpretation, redaction overclaiming, decontextualized case reuse, and translating history into operational instructions, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: historical modules use declassified or public records for analysis and governance lessons only; they do not reconstruct live tactics, sources, methods, or current field procedures.

43.1.4 Israeli and Continental Services core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 43; [266, 2026].

Term	Working definition
Declassification context	the release channel, date, and limits of an official historical source
Redaction caveat	the warning that missing text may change interpretation
Institutional lesson	the durable governance or analytic principle drawn from a case
Presentism	the error of forcing modern assumptions onto a historical record
Modern analogy	a bounded comparison that preserves differences between eras
Oversight failure	a documented breakdown in review, records, or accountability visible in the archive
Source-protection lesson	the historical principle about protecting people and methods without reconstructing live tradecraft
Declassified source-protection and…	Key terms: Declassified, protection, institutional.
Declassified cover-identity and…	Key terms: Declassified, cover, identity.

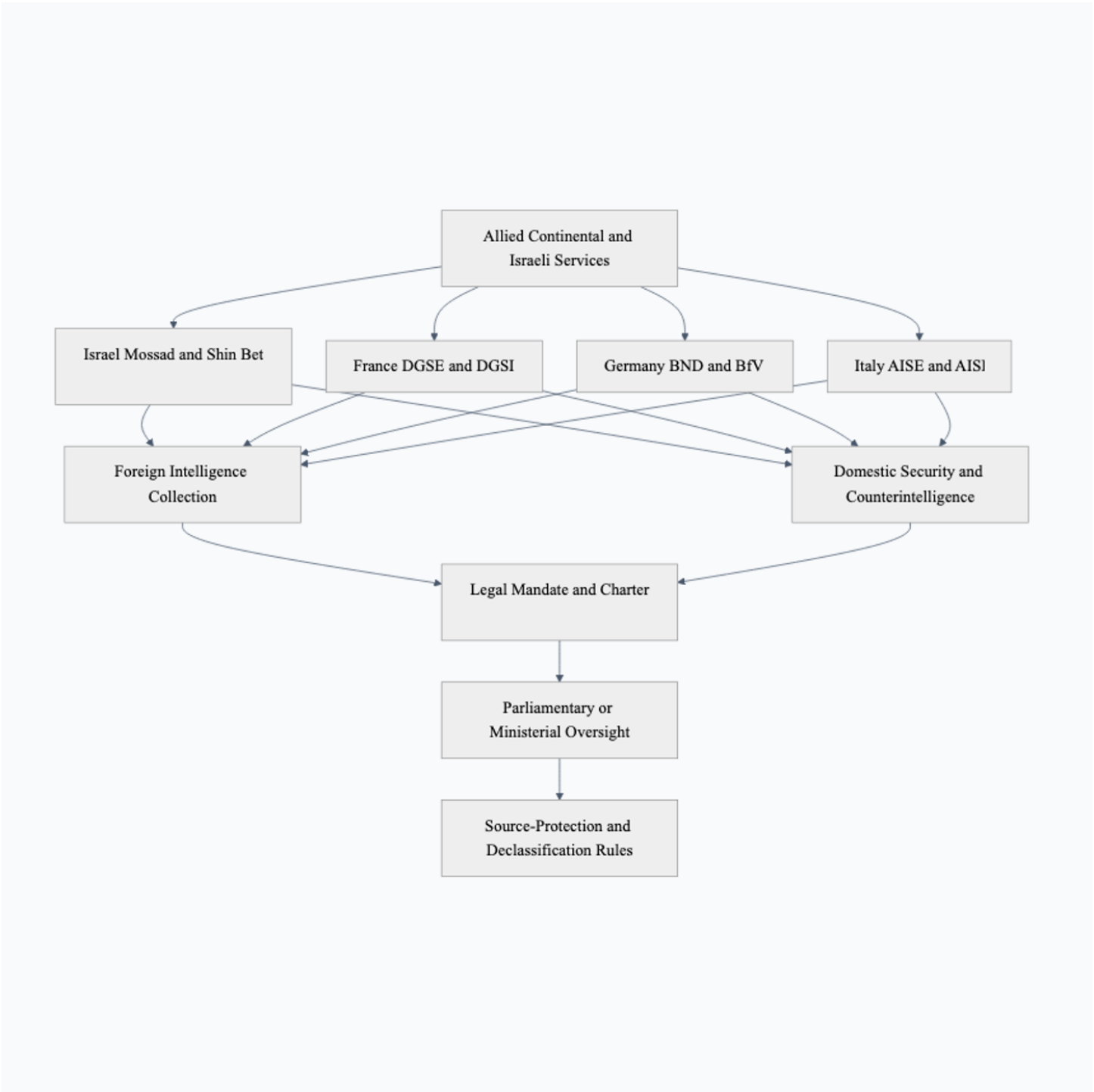


Figure 84: A comparative organizational view of allied continental and Israeli intelligence services showing the shared split between foreign collection, domestic security, and the oversight bodies that govern them. Its reader value is to make Allied Continental and Israeli Services, Israel Mossad and Shin Bet, France DGSE and DGSI, and Germany BND and BfV visible at a glance, with the historical intelligence services / israeli and continental services section as the source section and defensive review as the boundary.

43.2 Historical Case-Translation Lens path for Israeli and Continental Services: lesson cluster, safe artifact, and review

Evidence anchor. Section 43; [266, 2026].

43.2.1 Israeli and Continental Services practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 43; [266, 2026].

43.2.2 Israeli and Continental Services topic lessons: source-backed concepts and transfer tasks

This module builds historical intelligence study as declassified evidence review: archives teach institutional lessons when provenance, redaction, context, and modern boundaries are explicit. The sequence opens with **Declassified source-protection and institutional-control case study**, **Declassified cover-identity and source-protection case**, **Declassified covert-action oversight and source-protection case** and applies the **Historical Case-Translation Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 79; module overview Section 43; curriculum atlas Section 2.

Triangulation anchors. In module 30's topic-lessons section, directly verified anchors for the **Historical and Declassified Intelligence Services** lane include [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]; [Archives and Administration, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

43.2.2.1 Lesson 1: Declassified source-protection and institutional-control case study

Concept. Declassified source-protection and institutional-control case study studies the declassified record for institutional lessons about oversight, source protection, and limits on translating history into practice.

Why it matters. Declassified source-protection connects classroom vocabulary to Historical and Declassified Intelligence Services practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Declassified source-protection and institutional-control case study rests on [008, 2026]. The lead source's own note reads: An EBSCO Research Starter reference article on the Mossad, Israel's national intelligence agency established in 1949 and responsible for foreign intelligence collection and counterterrorism operations conducted outside Israel's borders. Use it for the working definition that **Declassified source-protection and institutional-control case study** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. For **Declassified source-protection**, reason from the sources cited in this row. [008, 2026] An EBSCO Research Starter reference article on the Mossad, Israel's national intelligence agency established in 1949 and responsible for foreign intelligence collection and counterterrorism operations conducted outside Israel's borders. It describes the agency's departmental structure (collection, political action and liaison, research, technology) and reviews historically documented operations including the 1960 capture of Adolf Eichmann and the rescue of Ethiopian Jews. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Declassified source-protection**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **Declassified source-protection and institutional-control case**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape **Declassified source-protection** work as a **declassified case-to-principle card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Transfer **Declassified source-protection** from this module to a second motif by preserving declassified-source interpretation and case-to-principle translation, replacing action with audit, and naming the blocked use.

43.2.2.2 Lesson 2: Declassified cover-identity and source-protection case

Concept. Declassified cover-identity and source-protection case treats agents as software actors with explicit permissions, logs, stop conditions, and human approval—not autonomous decision makers.

Why it matters. Analysts use **Declassified cover-identity** to separate historical lesson from reconstruction of live tactics or current sources and methods. A defensible treatment names the judgment it enables for declassified-source interpretation and case-to-principle translation review, the proof limit that romanticized tradecraft would otherwise hide, and the reviewer accountable for challenge.

Source support. Declassified cover-identity and source-protection case rests on [136, 2026]. Its anchor reference records: The Mossad is concerned with foreign intelligence gathering, intelligence analysis. Use it for fixing what **Declassified cover-identity and source-protection case** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. Ground **Declassified cover-identity** in the evidence the row cites. [136, 2026] The Mossad is concerned with foreign intelligence gathering, intelligence analysis. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. Build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **Declassified cover-identity**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape this subject work as a **declassified case-to-principle card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Reuse the **Declassified cover-identity** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

43.2.2.3 Lesson 3: Declassified covert-action oversight and source-protection case

Concept. Declassified covert-action oversight and source-protection case studies influence doctrine as audience analysis, message integrity, and ethics—not as manipulation technique.

Why it matters. Analysts use **Declassified covert-action oversight** to separate historical lesson from reconstruction of live tactics or current sources and methods. A defensible treatment names the judgment it enables for declassified-source interpretation and case-to-principle translation review, the proof limit that romanticized tradecraft would otherwise hide, and the reviewer accountable for challenge.

Source support. Declassified covert-action oversight and source-protection case rests on [297, 2026] and [298, 2026]. The most specific cited work observes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for the working definition that **Declassified covert-action oversight and source-protection case** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. For **Declassified covert-action oversight**, work from the cited evidence behind this row. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and

accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Declassified covert-action oversight**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **Declassified covert-action oversight and source-protection**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape **Declassified covert-action oversight** work as a **declassified case-to-principle card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Apply this module's safe boundary for **Declassified covert-action oversight** to another artifact while keeping declassified-source interpretation and case-to-principle translation and reviewer ownership explicit.

43.2.2.4 Lesson 4: Unit: Declassified source-protection and institutional-control case study

Concept. Unit: Declassified source-protection and institutional-control case study frames SIGINT as authority-bound collection with minimization, handling rules, and communications-security implications.

Why it matters. Analysts use **Unit: Declassified source-protection and institutional-control case study** to separate historical lesson from reconstruction of live tactics or current sources and methods. A defensible treatment names the judgment it enables for declassified-source interpretation and case-to-principle translation review, the proof limit that romanticized tradecraft would otherwise hide, and the reviewer accountable for challenge.

Source support. Unit: Declassified source-protection and institutional-control case study rests on [297, 2026] and [298, 2026]. The closest source to this row notes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for pinning down the scope of **Unit: Declassified source-protection and institutional-control case study**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. For **Unit: Declassified source-protection and institutional-control case study**, reason from the sources cited in this row. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Unit**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **Unit**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape **Unit: Declassified source-protection and institutional-control case study** work as a **declassified case-to-principle card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Transfer **Unit: Declassified source-protection and institutional-control case study** from this module to a second motif by preserving declassified-source interpretation and case-to-principle translation, replacing action with audit, and naming the blocked use.

43.2.2.5 Lesson 5: SDECE/DGSE: Declassified source-protection and institutional-control case study

Concept. SDECE/DGSE: Declassified source-protection and institutional-control case study studies the declassified record for institutional lessons about source protection, oversight, and the danger of translating historical methods into current practice.

Why it matters. SDECE/DGSE connects classroom vocabulary to Historical and Declassified Intelligence Services practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. SDECE/DGSE: Declassified source-protection and institutional-control case study rests on [297, 2026] and [298, 2026]. The most specific cited work observes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for the working definition that **SDECE/DGSE: Declassified source-protection and institutional-control case study** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. For **SDECE/DGSE**, reason from the sources cited in this row. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **SDECE/DGSE**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **SDECE/DGSE**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape **SDECE/DGSE** work as a **declassified case-to-principle card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Reuse the **SDECE/DGSE** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

43.2.2.6 Lesson 6: BND: Declassified source-protection and institutional-control case study

Concept. BND: Declassified source-protection and institutional-control case study studies the declassified record for institutional lessons about source protection, oversight, and the danger of translating historical methods into current practice.

Why it matters. BND: Declassified source-protection and institutional-control case study matters in the **Historical and Declassified Intelligence Services** lane because declassified-source interpretation and case-to-principle translation evidence must stay separate from judgment; romanticized tradecraft is a common failure.

Source support. BND: Declassified source-protection and institutional-control case study rests on [297, 2026] and [298, 2026]. The lead source's own note reads: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for the working definition that **BND: Declassified source-protection and institutional-control case study** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. For **BND: Declassified source-protection and institutional-control case study**, work from the cited evidence behind this row. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alterna-

tives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **BND**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **BND**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape **BND: Declassified source-protection and institutional-control case study** work as a **declassified case-to-principle card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Reuse the **BND: Declassified source-protection and institutional-control case study** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

43.2.2.7 Lesson 7: Stasi: Declassified source-protection and institutional-control case study

Concept. Stasi: Declassified source-protection and institutional-control case study studies the declassified record for institutional lessons about source protection, oversight, and the danger of translating historical methods into current practice.

Why it matters. Analysts use **Stasi: Declassified source-protection and institutional-control case study** to separate historical lesson from reconstruction of live tactics or current sources and methods. A defensible treatment names the judgment it enables for declassified-source interpretation and case-to-principle translation review, the proof limit that romanticized tradecraft would otherwise hide, and the reviewer accountable for challenge.

Source support. Stasi: Declassified source-protection and institutional-control case study rests on [297, 2026] and [298, 2026]. The most specific cited work observes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for pinning down the scope of **Stasi: Declassified source-protection and institutional-control case study**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Agency, 2026a]; [Agency, 2026h].

Evidence to inspect. For **Stasi: Declassified source-protection and institutional-control case study**, reason from the sources cited in this row. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Stasi**, build a **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** for this declassified-source interpretation and case-to-principle translation topic. The artifact must cite the declassified source descriptor, the bounded lesson about **Stasi**, the redaction caveat, the attribution uncertainty, the protected-detail boundary, and the reviewer who clears release. Shape **Stasi: Declassified source-protection and institutional-control case study** work as a **declassified case-to-principle card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

Transfer task. Transfer **Stasi: Declassified source-protection and institutional-control case study** from this module to a second motif by preserving declassified-source interpretation and case-to-principle translation, replacing action with audit, and naming the blocked use.

43.2.3 Israeli and Continental Services worked safe example: synthetic inputs, evidence, and review

Worked example: a sample seminar studies a declassified reform episode and extracts an oversight lesson without reconstructing current sources and methods. [266, 2026]; [267, 2026].

Triangulation anchors. In module 30's worked-example section, directly verified anchors for the **Historical and Declassified Intelligence Services** lane include [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]; [Archives and Administration, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **declassified-source interpretation**. Learners use a **declassified case-to-principle card** and keep this boundary visible: No current sources-and-methods reconstruction, operational emulation, or tactical transfer.

Frame. The classroom question centers on **Declassified source-protection and institutional-control case study**. Excluded actions stay explicit, and the **Historical Case-Translation Lens** planning question is: Which declassified source, release context, institutional lesson, and modern boundary can be carried forward without recreating operations?

Inputs. For the **Declassified source-protection and institutional-control case study** scenario, use public archive metadata, a short excerpt, a timeline template, and an oversight-question worksheet. The Historical Case-Translation Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Declassified source-protection and institutional-control case study**, students record provenance, mark redactions, build timeline, distinguish known from unknown, and extract a governance lesson. Pause whenever an inference about Declassified source-protection and institutional-control case study appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Declassified source-protection and institutional-control case study** classroom scenario; unit artifact = declassified case-to-principle card; evidence = allowed inputs; method = declassified-source interpretation and case-to-principle translation; output = a historical case card with release context, caveats, lesson, and evidence-bounded boundary; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Declassified source-protection and institutional-control case study** as "Historical Case-Translation Lens confirms it" is not enough. The revision ties the claim to declassified-source interpretation and case-to-principle translation, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Declassified source-protection and institutional-control case study** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

43.2.4 Israeli and Continental Services practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Historical Case-Translation Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**.

Triangulation anchors. In module 30's practice-sequence section, directly verified anchors for the **Historical and Declassified Intelligence Services** lane include [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]; [Archives and Administration, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Declassified source-protection and institutional-control case study, Declassified cover-identity and source-protection case, Declassified covert-action oversight and source-protection case; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Historical and Declassified Intelligence Services** lane.
2. Frame	Answer the lens question: Which declassified source, release context, institutional lesson, and modern boundary can be carried forward without recreating operations?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Declassified source-protection and institutional-control case study: historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the declassified case-to-principle card fields for Declassified source-protection and institutional-control case study.	Unit profile note.	Evidence artifacts include release metadata, redaction caveat.
4. Challenge	Test the misconception that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.	Failure-mode note.	The artifact applies the key distinction: separate historical lesson from reconstruction of live tactics or current sources and methods.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

43.2.4.1 Israeli and Continental Services instructor notes: source reasoning, review points, and studio focus Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**. [266, 2026]; [267, 2026].

43.2.4.2 Israeli and Continental Services extension exercise: peer validation and refresh trigger review **Evidence anchor.** Section 43; [266, 2026].

Have learners swap artifacts and apply the **Historical Case-Translation Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**.

43.2.5 Israeli and Continental Services knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 43; [266, 2026].

1. Explain how **Declassified source-protection and institutional-control case study** is defined here; name the source descriptor that supports the definition.
2. Contrast **Declassified source-protection and institutional-control case study** with **Declassified cover-identity and source-protection case** using the **Historical Case-Translation Lens** artifact fields.
3. Identify one failure mode from the **Historical and Declassified Intelligence Services** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which institutional lesson is defensible from the record, and which claim reconstructs live tradecraft?
5. Correct this misconception: that a source identity is safe to discuss once the operation is historical, when protection obligations and re-identification risk outlast the case itself.

43.2.5.1 Israeli and Continental Services answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Declassified source-protection and institutional-control case study** without source evidence, uncertainty, or a safe transfer task.

43.3 Israeli and Continental Services assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 43; [266, 2026].

43.3.1 Israeli and Continental Services evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 43; [266, 2026].

43.3.2 Israeli and Continental Services transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 43; [266, 2026].

43.3.2.1 Israeli and Continental Services lineage and source tradition: profile, concepts, and first anchors This sits in the **Historical and Declassified Intelligence Services** lineage: turning declassified records and official histories into safe institutional lessons about analytic judgment, secrecy, oversight, technical-intelligence evolution, and reform. [266, 2026]; [267, 2026].

43.3.2.2 Israeli and Continental Services working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 43; [266, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**, with provenance and reviewability throughout.

43.3.2.3 Israeli and Continental Services knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [266, 2026]; [267, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

43.3.2.4 Israeli and Continental Services transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 43; [266, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**.
- **Evidence contract:** keep the **Historical and Declassified Intelligence Services** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

43.3.2.5 Israeli and Continental Services profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 43; [266, 2026].

The matched profile emphasizes turning declassified records and official histories into safe institutional lessons about analytic judgment, secrecy, oversight, technical-intelligence evolution, and reform. The method stack is provenance review, declassification-status notation, institutional timeline building, case-to-principle translation, and uncertainty about redacted records; the local topic cluster is **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**.

43.3.3 Israeli and Continental Services evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 43; [266, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Historical and Declassified Intelligence Services** profile tells reviewers what evidence is strong enough for the module artifact built around **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**.

43.3.3.1 Israeli and Continental Services guide source spine: inherited keys and local citation roles Primary guide citations: [266, 2026]; [267, 2026]; [271, 2026]; [274, 2026]; [278, 2026]; [280, 2026]; [287, 2026]; [288, 2026]; [295, 2026]; [008, 2026]; [136, 2026]; [297, 2026]; [298, 2026].

43.3.3.2 Israeli and Continental Services verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [266, 2026]; [267, 2026].

Tier	What counts	How it is used
Source guide	[266, 2026]; [267, 2026]; [271, 2026]; [274, 2026]; [278, 2026]; [280, 2026]; [287, 2026]; [288, 2026]; [295, 2026]; [008, 2026]; [136, 2026]; [297, 2026]; [298, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 30's source-canon section, directly verified anchors for the **Historical and Declassified Intelligence Services** lane include [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]; [Archives and Administration, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case** and [266, 2026]; [267, 2026], but only directly verified source URLs are encoded as citations.

43.3.3.3 Israeli and Continental Services intelligence practice lens: evidence artifact and safety check Practice lens: **Historical Case-Translation Lens** for **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**. [266, 2026]; [267, 2026].

Planning question: Which declassified source, release context, institutional lesson, and modern boundary can be carried forward without recreating operations?

Evidence artifact: historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary.

Validation rule: distinguish what the record shows, what remains redacted or unknown, and which governance lesson is defensibly transferable. Applied to **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**.

Handoff contract: handoff preserves archive citation, historical context, analytic lesson, oversight implication, and modern analogy as separate fields.

Safety check: exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material.

43.3.3.4 Israeli and Continental Services runtime-to-reader map: generated sections and verifier surfaces **Evidence anchor.** Section 43; [266, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	30.99	30.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Israeli and Continental Services to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Bounded autonomy, procurement, incident-response, and assurance studio	30.101	30.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Israeli and Continental Services	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Model-card, recoverability, retention, and learner-support evidence package	30.102	30.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Israeli and Continental Services	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified source-protection and institutional-control case study	30.1	30.1 source title transformed into safe curriculum treatment; original: Mossad: Structure, Culture, Notable Operations	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Declassified cover-identity and source-protection case	30.2	30.2 source title transformed into safe curriculum treatment; original: Eli Cohen: Deep Cover Agent in Syria	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified covert-action oversight and source-protection case	30.3	30.3 source title transformed into safe curriculum treatment; original: Operation Wrath of God: PSYOP and Targeted Killing	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified source-protection and institutional-control case study	30.4	30.4 source title transformed into safe curriculum treatment; original: Unit 8200: SIGINT, AI, and Cyber Excellence	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified source-protection and institutional-control case study	30.5	30.5 source title transformed into safe curriculum treatment; original: SDECE/DGSE: French Intelligence Tradition	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified source-protection and institutional-control case study	30.6	30.6 source title transformed into safe curriculum treatment; original: BND: German Federal Intelligence Service	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified source-protection and institutional-control case study	30.7	30.7 source title transformed into safe curriculum treatment; original: Stasi: East German Pervasive Domestic Intelligence	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material

43.3.3.5 Israeli and Continental Services reusable subsection contract: topic rows, artifacts, and safety duties **Evidence anchor.** Section 43; [266, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Declassified source-protection and institutional-control case study	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified cover-identity and source-protection case	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Declassified covert-action oversight and source-protection case	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Unit: Declassified source-protection and institutional-control case study	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
SDECE/DGSE: Declassified source-protection and institutional-control case study	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
BND: Declassified source-protection and institutional-control case study	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material
Stasi: Declassified source-protection and institutional-control case study	Historical Case-Translation Lens	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary	exclude reconstruction of current sources, methods, tactics, cover, or collection workflows from historical material

43.3.3.6 Israeli and Continental Services annotated source ledger: real titles and local contribution Each source cited by this **Historical and Declassified Intelligence Services** module is paired below with its real title and a one-line note on what it contributes to **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**.

Source	Cited work	What it contributes	Status
[266, 2026]	PROV Overview	A W3C Working Group Note from 2013 that provides an overview and roadmap for the PROV family of specifications for representing and exchanging provenance information on the web. It defines provenance as information about the entities, activities, and people involved in producing data, used to assess quality, reliability, and trustworthiness.	verified source-guide
[267, 2026]	PROV-O: The PROV Ontology	The W3C Recommendation for PROV-O, published in April 2013, which expresses the PROV data model as an OWL2 ontology for representing provenance information across systems. It defines three core classes, Entity, Activity, and Agent, and organizes terms into starting-point, expanded, and qualified categories.	verified source-guide
[271, 2026]	DataCite Metadata Schema	The DataCite Metadata Schema page, introducing a standardized framework of core metadata properties chosen for accurate and consistent identification of research resources for citation and retrieval. It notes the latest version, 4.7 (March 2026), which adds resource types such as Poster and Presentation along with new identifier and relation-type options.	verified source-guide
[274, 2026]	CAST Universal Design for Learning Guidelines version 3.0	The official CAST website for the Universal Design for Learning (UDL) Guidelines version 3.0, released in 2024. The framework offers research-based guidance for designing inclusive learning environments and is organized around three principles: Engagement (motivation and emotional support), Representation (accessible presentation of information), and Action and Expression (diverse means of participation and communication).	verified source-guide
[278, 2026]	Recommendation of the Council on Public Procurement	The OECD Recommendation of the Council on Public Procurement (OECD/LEGAL/0411), a legal instrument adopted by the OECD Council in 2015 on the proposal of the Public Governance Committee. It frames public procurement as a pillar of strategic governance and service delivery and sets out principles for governments to follow.	verified source-guide
[280, 2026]	NIST SP 800-61 Rev. 3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management	NIST SP 800-61 Rev. 3, published April 2025, integrates incident response guidance into broader cybersecurity risk management aligned with the NIST Cybersecurity Framework 2.0, superseding the 2012 Rev. 2. The publication addresses cyber threat information sharing, incident handling and management practices, and procedures for detecting, responding to, and recovering from security incidents.	verified source-guide

Source	Cited work	What it contributes	Status
[287, 2026]	Datasheets for Datasets	A 2018 arXiv paper proposing 'datasheets for datasets,' a standardized documentation framework for machine learning datasets modeled on electronic component datasheets. The authors argue the field lacks consistent dataset documentation, which creates risk in high-stakes applications, and propose that datasets be accompanied by documentation covering motivation, composition, collection process, recommended uses, and test results.	verified source-guide
[288, 2026]	Algorithmic Transparency Recording Standard Hub	A GOV.UK collection page serving as the hub for the UK Algorithmic Transparency Recording Standard (ATRS), maintained by the Government Digital Service. It provides a standardized template for documenting public-sector use of algorithmic tools, completion guidance, policy on scope and compliance, and a searchable repository of published transparency records.	verified source-guide
[295, 2026]	M-25-22: Driving Efficient Acquisition of Artificial Intelligence in Government	OMB Memorandum M-25-22 (April 3, 2025), Driving Efficient Acquisition of Artificial Intelligence in Government, issued under Executive Order 13960 and related directives. It provides guidance to federal agencies for acquiring effective and trustworthy AI in a timely, cost-effective manner, and rescinds and replaces earlier memorandum M-24-18.	verified source-guide
[008, 2026]	Mossad / Military History and Science	An EBSCO Research Starter reference article on the Mossad, Israel's national intelligence agency established in 1949 and responsible for foreign intelligence collection and counterterrorism operations conducted outside Israel's borders. It describes the agency's departmental structure (collection, political action and liaison, research, technology) and reviews historically documented operations including the 1960 capture of Adolf Eichmann and the rescue of Ethiopian Jews.	verified source-guide
[136, 2026]	Mossad's secretive operations and reputation - Facebook	The Mossad is concerned with foreign intelligence gathering, intelligence analysis.	original source-guide
[297, 2026]	Intelligence Community Directive 203: Analytic Standards	Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products.	original source-guide
[298, 2026]	Intelligence Community Directives	Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations.	original source-guide

Where this sits. This module's overview is Section 43; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

43.3.4 Israeli and Continental Services governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 43; [266, 2026].

43.3.5 Israeli and Continental Services analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 30's governance-boundary section, directly verified anchors for the **Historical and Declassified Intelligence Services** lane include [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]; [Archives and Administration, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Research lane: **Historical and Declassified Intelligence Services** for **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**. [266, 2026]; [267, 2026].
Curriculum topic spine: Declassified source-protection and institutional-control case study, **Declassified cover-identity and source-protection case**, **Declassified covert-action oversight and source-protection case**. **Verified anchor cluster:** [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]; [Archives and Administration, 2026b]; [of the Director of National Intelligence, 2026e]; [Jr., 2007]; [Agency, 2009].
Conceptual depth: turning declassified records and official histories into safe institutional lessons about analytic judgment, secrecy, oversight, technical-intelligence evolution, and reform.
Method stack: provenance review, declassification-status notation, institutional timeline building, case-to-principle translation, and uncertainty about redacted records.
Composability contract: archive source, release channel, historical context, analytic lesson, oversight implication, and modern analogy remain explicitly separated.
Known failure modes: romanticized tradecraft, presentist interpretation, redaction overclaiming, decontextualized case reuse, and translating history into operational instructions.
Defensive boundary: historical modules use declassified or public records for analysis and governance lessons only; they do not reconstruct live tactics, sources, methods, or current field procedures. Applied to **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**.

Anchor	Why it matters here
[Agency, 2026a]	Official CSI landing page for Studies in Intelligence, declassified professional reflection, analytic history, and institutional learning. Checked as of 2026-05-21; role: curriculum_anchor.
[Agency, 2026h]	Official declassified historical-release library for cryptologic history, SIGINT history, COMSEC, oral histories, and historical cases. Checked as of 2026-05-21; role: curriculum_anchor.
[Office, 2026a]	Official declassified satellite-reconnaissance program archive for CORONA, GAMBIT, POPPY, QUILL, and other historical technical-intelligence cases. Checked as of 2026-05-21; role: curriculum_anchor.
[Archives and Administration, 2026b]	Official NARA guide to CIA Record Group 263, archival provenance, record series, and declassified intelligence research pathways. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026e]	Official ODNI explanation of analytic objectivity, ombuds, and tradecraft standards. Checked as of 2026-05-21; role: curriculum_anchor.
[Jr., 2007]	Foundational analytic cognition source for bias, mental models, and structured reasoning. Checked as of 2026-06-06; role: curriculum_anchor.
[Agency, 2009]	Official structured analytic techniques primer for bias checks, alternatives, and warning analysis. Checked as of 2026-05-21; role: curriculum_anchor.

43.3.5.1 Israeli and Continental Services evidence standard and citation floor: source families and discovery limits Official guidance supplies governance, safety, and legal constraints for the **Historical and Declassified Intelligence Services** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [266, 2026]; [267, 2026].

43.3.6 Israeli and Continental Services agentic boundary: assist, approve, block, and record

Evidence anchor. Section 43; [266, 2026].
AGEINT translation is bounded by the **Historical and Declassified Intelligence Services** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**.

43.3.6.1 Israeli and Continental Services permitted defensive utility: curriculum uses and safe outputs **Evidence anchor.** Section 43; [266, 2026].
The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**.

43.3.6.2 Israeli and Continental Services excluded operational boundary: blocked actions and stop rules Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [266, 2026]; [267, 2026] and **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

43.3.7 Israeli and Continental Services governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 43; [266, 2026].
Governance is practiced as a gate on the **Historical and Declassified Intelligence Services** lane. Learners use the **Historical Case-Translation Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact

must stop for human review while using **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**.

43.3.7.1 Israeli and Continental Services governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [266, 2026]; [267, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Historical and Declassified Intelligence Services** failure modes and the **Historical Case-Translation Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

43.3.7.2 Israeli and Continental Services evidence package handoff: appendices, records, and reuse

Evidence anchor. Section 43; [266, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Historical Case-Translation Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**.

43.3.7.3 Israeli and Continental Services current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**. [266, 2026]; [267, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_cia_center_for_study_of_intelligence` for **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**?	Center for the Study of Intelligence; lane `historical_declassified_sources`; checked 2026-05-21.	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary; Official CSI landing page for Studies in Intelligence, declassified professional reflection, analytic history, and institutional learning.
What does the module inherit from `official_nsa_historical_releases` for **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**?	NSA Historical Releases; lane `historical_declassified_sources`; checked 2026-05-21.	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary; Official declassified historical-release library for cryptologic history, SIGINT history, COMSEC, oral histories, and historical cases.
What does the module inherit from `official_nro_declassified_programs` for **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**?	Declassified NRO Programs and Projects; lane `historical_declassified_sources`; checked 2026-05-21.	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary; Official declassified satellite-reconnaissance program archive for CORONA, GAMBIT, POPPY, QUILL, and other historical technical-intelligence cases.
What does the module inherit from `official_nara_cia_records` for **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**?	Records of the Central Intelligence Agency; lane `historical_declassified_sources`; checked 2026-05-21.	historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary; Official NARA guide to CIA Record Group 263, archival provenance, record series, and declassified intelligence research pathways.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 43; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

43.3.8 Israeli and Continental Services assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 43; [266, 2026].

43.3.9 Israeli and Continental Services assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 43; [266, 2026].

43.3.9.1 Israeli and Continental Services capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case** and [266, 2026]; [267, 2026].

43.3.9.2 Israeli and Continental Services instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case** and [266, 2026]; [267, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

43.3.9.3 Israeli and Continental Services assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Declassified source-protection and institutional-control case study	Completed **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Declassified cover-identity and source-protection case	Completed **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Declassified covert-action oversight and source-protection case	Completed **historical case card with provenance, redaction caveats, timeline, lesson, and evidence-bounded boundary** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

43.3.10 Israeli and Continental Services refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [266, 2026]; [267, 2026] and **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**.

43.3.10.1 Israeli and Continental Services refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**. The local signals begin with [266, 2026]; [267, 2026].

43.3.10.2 Israeli and Continental Services claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**, and the source spine for these checks begins with [266, 2026]; [267, 2026].

43.3.11 Israeli and Continental Services reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [266, 2026]; [267, 2026].

Triangulation anchors. In module 30's review-checklist section, directly verified anchors for the **Historical and Declassified Intelligence Services** lane include [Agency, 2026a]; [Agency, 2026h]; [Office, 2026a]; [Archives and Administration, 2026b]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case**. [266, 2026]; [267, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

43.3.12 Israeli and Continental Services learning-path links: module map, overview, and curriculum atlas

These links keep **Declassified source-protection and institutional-control case study; Declassified cover-identity and source-protection case** paired with the orientation atlas, the parent unit, and the previous and next modules, so a reader can trace which claims and caveats are inherited rather than re-derived here. Anchored at [266, 2026]; [267, 2026].

Section 2, Section 39, Section 42, Section 44

44 AGEINT — AGENTIC INTELLIGENCE

44.1 AGEINT — AGENTIC INTELLIGENCE learning spine and source route: unit purpose, module order, and evidence handoff

Evidence anchor. Section 44; [232, 2026].

44.1.1 governed agentic intelligence discipline spine: domain question and learning focus

Evidence anchor. Section 44; [232, 2026].
This unit teaches **governed agentic intelligence**. AGEINT lessons treat agents as bounded delegated systems whose identity, tools, memory, logs, stop conditions, and review gates define safe use.

44.1.2 governed agentic intelligence source-use contract: citation roles and evidence limits

Evidence anchor. Section 44; [232, 2026].
Use MCP, AI assurance, secure-development, and public-sector agentic AI anchors for tool boundaries, interoperability, external-memory governance, and oversight claims; use domain-specific agent-memory or cognitive literature for memory taxonomy claims.

44.1.3 governed agentic intelligence practice artifact: recurring packet and retained evidence

Evidence anchor. Section 44; [232, 2026].
The recurring practice artifact is a **agent run and assurance card** that draws on tool-allowlist record, external-memory governance boundary, blocked-action log, and recovery decision. The unit keeps its learning spine explicit. Learners design least-privilege agent roles, verify tool calls, distinguish claim/source memory from cognitive-memory taxonomy, record blocked actions, and define recovery.

44.1.4 governed agentic intelligence safety boundary: accountable, synthetic, and evidence-bounded limits

No autonomous external action, credentialed operations, live-target workflows, or uncontrolled tool use.
This unit introduces the part's governing question, evidence artifacts, source-support spine, and capstone thread before the individual modules begin. [232, 2026]; [235, 2026].
Learners carry one unit capstone thread through the part: define an accountable intelligence question, bind it to source-quality constraints, produce a reviewable artifact, test the artifact against failure modes, and hand it off with enough context for another analyst or instructor to audit. The capstone remains public, synthetic, or owned-lab throughout; its first source anchors are [232, 2026]; [235, 2026].
This unit's deliverables are a source-canon card, claim/evidence ledger, safe-practice lab packet, failure-mode note, instructor rubric, and debrief memo. The full source-lane and evidence-package ledgers appear in the orientation and appendices; this unit introduction keeps only the learner-facing spine for [232, 2026]; [235, 2026].
This unit's safety gates are scope authorization, rights review, data provenance, tool allowlisting, human oversight, rollback, and evidence-bounded output. A missing gate turns the activity into a tabletop, audit, or written governance exercise until the gate is restored against [232, 2026]; [235, 2026].
Capstone thread:

Phase	Artifact	Review gate
Question	accountable learning question and excluded-action list	instructor confirms scope, allowed data, and rights impact
Source canon	source-lane map with guide citations, verified anchors, and refresh dates	citation keys resolve and source identity lock remains stable
Evidence ledger	claim, evidence, uncertainty, confidence, and reviewer register	every material claim has a source, caveat, and owner
Safe lab	synthetic or public dataset packet, tool allowlist, and stop conditions	no live target, private data, external action, or unsafe cyber-physical step
Assurance	evaluation rubric, failure-mode drill, rights map, and remediation note	human reviewer signs off before presentation or reuse
Debrief	capstone memo with lessons, residual risk, refresh triggers, and handoff owner	all unresolved questions and future approvals are explicit

Research lane: Agentic AI Governance and Tool Security. Core anchors: [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]. Conceptual focus: delegated action under explicit authority, identity, permissions, tool boundaries, monitoring, and human escalation. Composability contract: agents, tools, credentials, memory, retrieval stores, policies, and logs remain separately inspectable and revocable components. **Practice lens:** Agentic Tool-Governance Lens; Which human authority, agent identity, tool permission, autonomy limit, incident threshold, and recoverability condition bounds the workflow? [232, 2026]; [235, 2026].

44.1.5 AGEINT — AGENTIC INTELLIGENCE visual navigation and module map: evidence flow, order, and safety cues

The unit uses Figure 85, Figure 86, and Figure 87 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 43, Section 45.

44.1.6 AGEINT — AGENTIC INTELLIGENCE module roster and source-lane inventory: citations, lanes, and learner route

Module	Section reference	Source spine
Foundations of AGEINT	Section 45	[232, 2026]; [235, 2026]; [247, 2026]; [279, 2026]; [282, 2026]; [284, 2026]; [289, 2026]; [291, 2026]; [296, 2026]; [137, 2026]; [138, 2026]; [139, 2026]; [140, 2026]; [141, 2026]; [142, 2026]; [004, 2026]; [005, 2026]; [299, 2026]; [306, 2026]; [312, 2026]; [301, 2026]; [298, 2026].

Module	Section reference	Source spine
AGEINT Design Patterns and Archetypes	Section 46	[233, 2026]; [258, 2026]; [272, 2026]; [275, 2026]; [276, 2026]; [283, 2026]; [286, 2026]; [293, 2026]; [295, 2026]; [143, 2026]; [139, 2026]; [144, 2026]; [145, 2026]; [146, 2026]; [147, 2026]; [148, 2026]; [138, 2026]; [004, 2026]; [149, 2026]; [150, 2026]; [076, 2026]; [151, 2026]; [152, 2026]; [137, 2026]; [299, 2026]; [306, 2026]; [312, 2026]; [297, 2026]; [298, 2026]; [309, 2026]; [310, 2026]; [300, 2026]; [304, 2026]; [303, 2026]; [305, 2026]; [302, 2026]; [301, 2026]; [307, 2026]; [308, 2026]; [311, 2026].
AGEINT Frameworks and Infrastructure	Section 47	[255, 2026]; [256, 2026]; [258, 2026]; [273, 2026]; [274, 2026]; [275, 2026]; [286, 2026]; [287, 2026]; [292, 2026]; [147, 2026]; [153, 2026]; [154, 2026]; [144, 2026]; [155, 2026]; [156, 2026]; [157, 2026]; [158, 2026]; [159, 2026]; [137, 2026]; [146, 2026]; [299, 2026]; [306, 2026]; [312, 2026].
AGEINT Security and Adversarial Considerations	Section 48	[234, 2026]; [235, 2026]; [236, 2026]; [276, 2026]; [277, 2026]; [284, 2026]; [288, 2026]; [289, 2026]; [293, 2026]; [147, 2026]; [155, 2026]; [159, 2026]; [137, 2026]; [160, 2026]; [161, 2026]; [100, 2026]; [162, 2026]; [004, 2026]; [148, 2026]; [299, 2026]; [306, 2026]; [312, 2026].
Active Inference and AGEINT	Section 49	[247, 2026]; [248, 2026]; [265, 2026]; [278, 2026]; [279, 2026]; [283, 2026]; [290, 2026]; [291, 2026]; [294, 2026]; [106, 2026]; [003, 2026]; [163, 2026]; [164, 2026]; [105, 2026]; [299, 2026]; [306, 2026]; [312, 2026]; [309, 2026]; [310, 2026]; [300, 2026].
AGEINT Python Code Library	Section 50	[242, 2026]; [243, 2026]; [246, 2026]; [280, 2026]; [281, 2026]; [282, 2026]; [292, 2026]; [295, 2026]; [296, 2026]; [299, 2026]; [306, 2026]; [312, 2026]; [309, 2026]; [310, 2026]; [300, 2026]; [304, 2026]; [303, 2026]; [305, 2026]; [307, 2026]; [301, 2026]; [298, 2026]; [308, 2026]; [311, 2026].

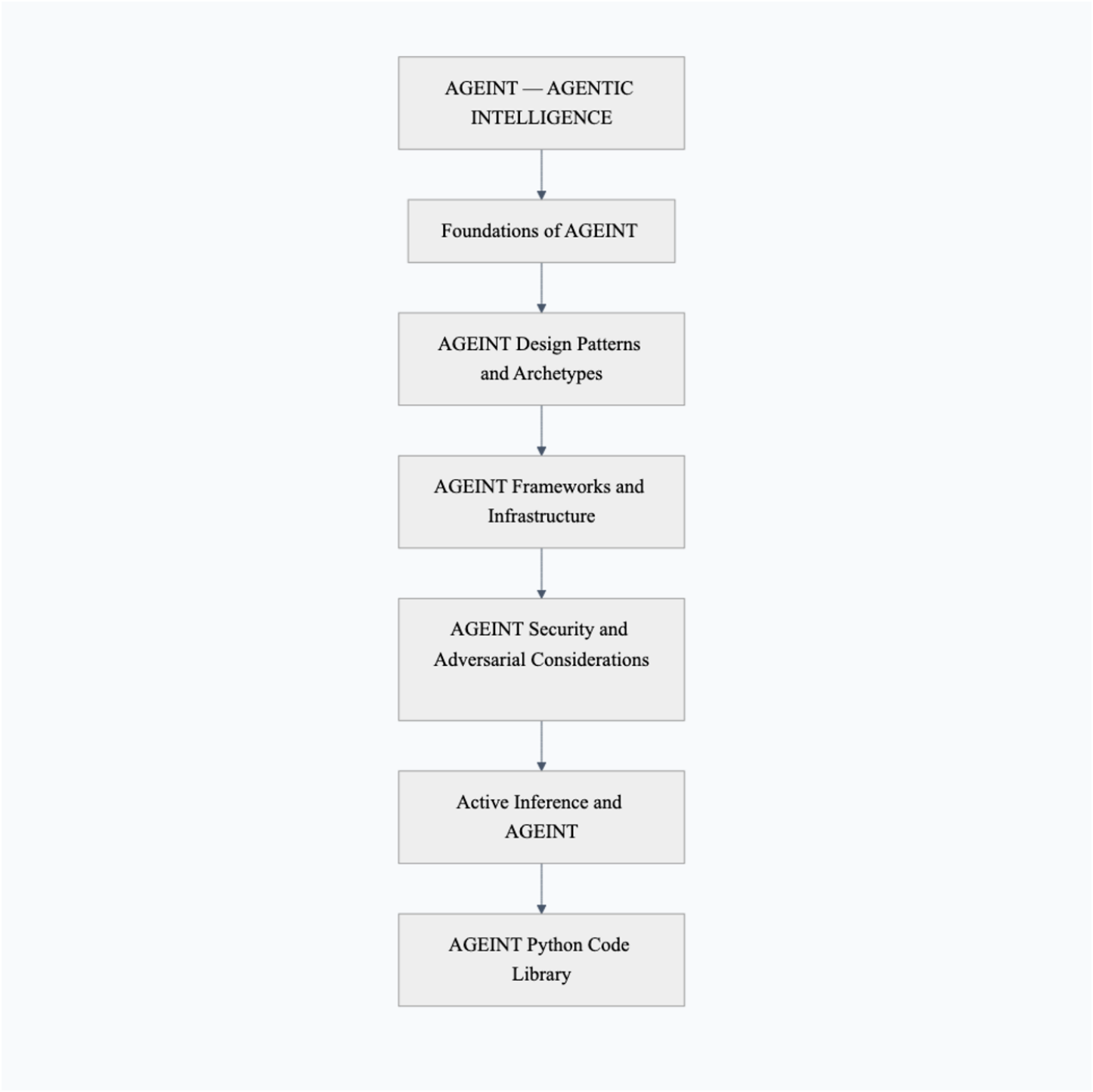


Figure 85: The unit module map traces the part's chapters as a linear reading sequence. Its reader value is to make 6 module nodes in the unit's ordered, source-backed reading sequence from its first module to its last visible at a glance, with the ageint agentic intelligence section as the source section and defensive review as the boundary.

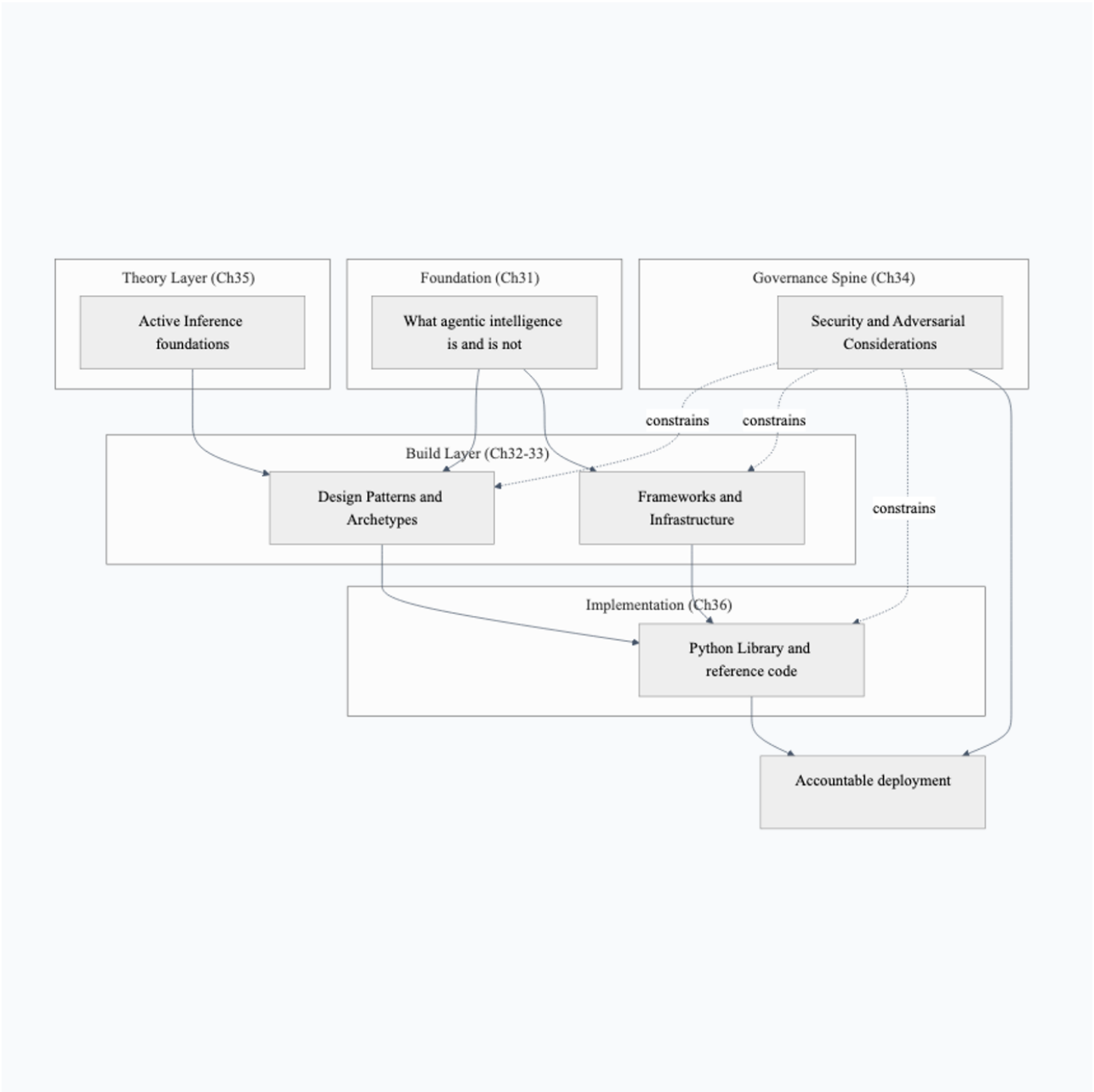


Figure 86: This part builds from foundations through design patterns, frameworks, and a Python library to accountable deployment, with security and adversarial considerations running as a governance spine that constrains every build layer. Its reader value is to make Foundation (Ch31), What agentic intelligence is and is not, Build Layer (Ch32-33), and Design Patterns and Archetypes visible at a glance, with the ageint agentic intelligence section as the source section and defensive review as the boundary.

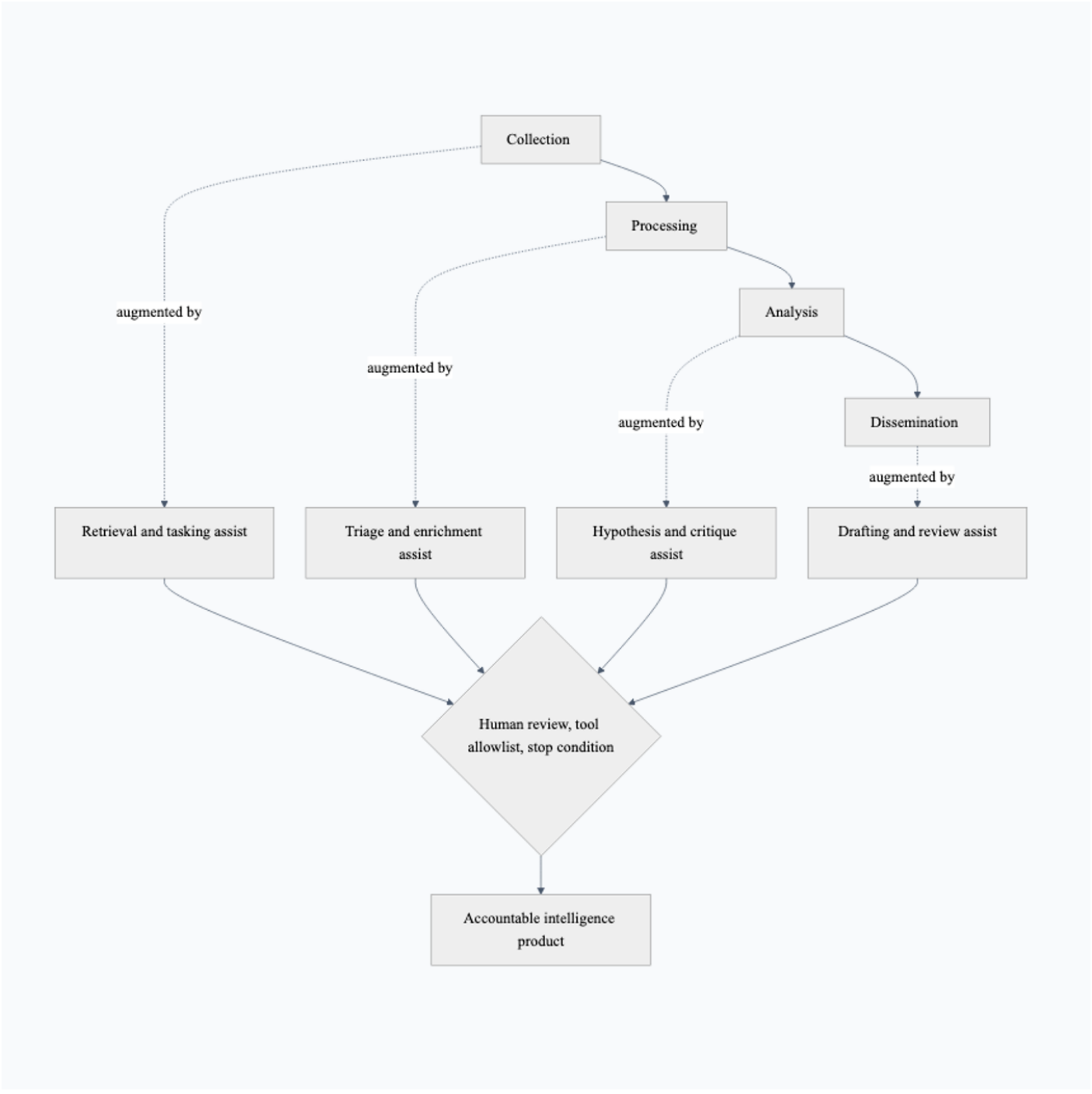


Figure 87: Conceptual/pedagogical schematic: AGEINT does not replace the intelligence cycle; it illustrates bounded assistance under human review, tool allowlists, and stop conditions. Its reader value is to make Collection, Retrieval and tasking assist, Processing, and Triage and enrichment assist visible at a glance, with the ageint agentic intelligence section as the source section and defensive review as the boundary.

45 Foundations of AGEINT

45.0.1 Foundations of AGEINT figures and course links: visual evidence, source flow, and navigation

The module uses Figure 88 and Figure 85 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 44, Section 46.
This module teaches the **Agentic AI Governance and Tool Security** lane through a bounded, source-backed coursebook chapter. [232, 2026]; [235, 2026].

45.1 Agentic AI Governance and Tool Security frame for Foundations of AGEINT: source context, topic focus, and reader task

Evidence anchor. Section 45; [232, 2026].

45.1.1 Foundations of AGEINT orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 45; [232, 2026].

45.1.2 Foundations of AGEINT conceptual primer: source context, core model, and reader task

This chapter teaches agentic AI as delegated action under control: identity, authority, tool permissions, memory, logs, stop conditions, and recoverability define what an agent may do. The chapter uses **Agentic Tool-Governance Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**.
The central distinction is to separate agent assistance from autonomous external action. Core topics include **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack; Unified Taxonomy: Perception → Brain → Planning → Action → Collaboration**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [232, 2026]; [235, 2026].
Learners move from vocabulary and the **Agentic Tool-Governance Lens** distinction through topic lessons on **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems** with evidence and misconception checks, then assemble an **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** with safety and rights gates.

45.1.3 Foundations of AGEINT learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 45; [232, 2026].

- Connect **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems and From LLMs to Agents: The Cognitive Controller Stack** to **Agentic AI Governance and Tool Security** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build an **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate agent assistance from autonomous external action; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as excessive agency, shadow tools, indirect prompt injection, memory poisoning, confused authority, and unbounded action chains, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: agentic workflows stay synthetic, owned-lab, supervised, logged, rate-limited, and reversible unless a lawful production authority exists.

45.1.4 Foundations of AGEINT core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 45; [232, 2026].

Term	Working definition
Agent identity	the named software actor, role, and authorization context for a run
Tool allowlist	the bounded set of actions the agent may request
Delegation	the handoff of a task under explicit human authority and review
Bounded autonomy	the documented ceiling on what an agent may decide or request without review
Recoverability	the path back to a known-safe state after a bad output or action request
AI incident	a logged event where an AI system creates or plausibly creates harm or loss of control
Prompt injection	untrusted content that attempts to override instructions or authority boundaries
Pattern registry	the catalog of approved agent behaviors, prompts, and evaluation hooks
Adversarial eval	structured tests that probe agent misuse, injection, and over-delegation before release
Defining AGEINT: From AI Agents to Autonomous…	Key terms: Defining, AGEINT, AI.
From LLMs to Agents: The Cognitive Controller…	Key terms: LLMs, Agents, Cognitive.

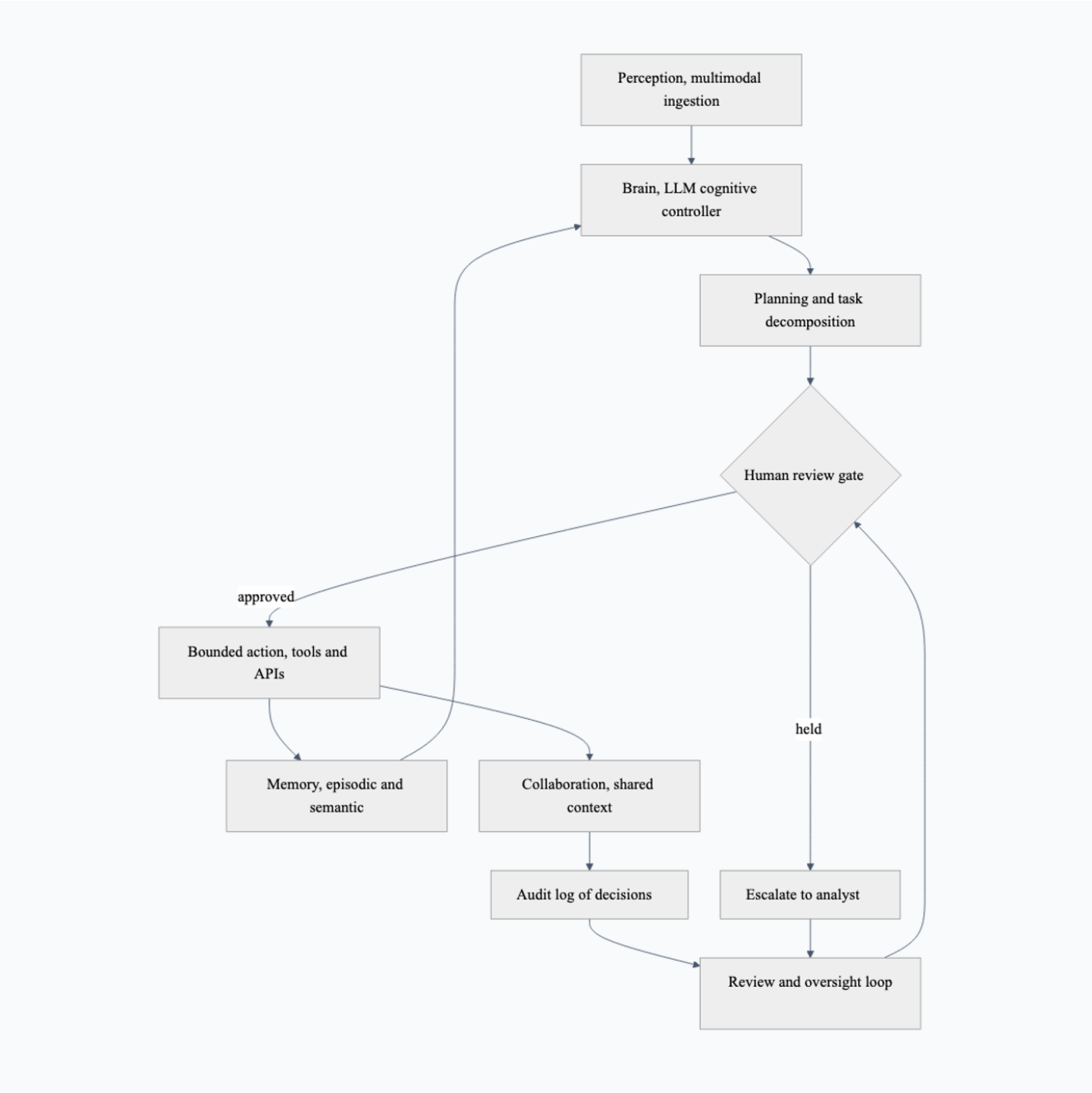


Figure 88: A conceptual view of how an agentic intelligence system layers perception, reasoning, memory, planning, and bounded action under continuous human oversight. In the ageint agentic intelligence / foundations of ageint section, it lets readers compare Perception, multimodal ingestion, Brain, LLM cognitive controller, Memory, episodic and semantic, and Planning and task decomposition so the visual functions as a traceable course aid rather than an unscoped assertion.

45.2 Agentic Tool-Governance Lens path for Foundations of AGEINT: lesson cluster, safe artifact, and review

Evidence anchor. Section 45; [232, 2026].

45.2.1 Foundations of AGEINT practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 45; [232, 2026].

45.2.2 Foundations of AGEINT topic lessons: source-backed concepts and transfer tasks

This module builds agentic AI as delegated action under control: identity, authority, tool permissions, memory, logs, stop conditions, and recoverability define what an agent may do. The sequence opens with **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems**, **From LLMs to Agents: The Cognitive Controller Stack**, **Unified Taxonomy: Perception → Brain → Planning → Action → Collaboration** and applies the **Agentic Tool-Governance Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 85; module overview Section 45; curriculum atlas Section 2.

Triangulation anchors. In module 31's topic-lessons section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

45.2.2.1 Lesson 1: Defining AGEINT: From AI Agents to Autonomous Intelligence Systems

Concept. Defining AGEINT: From AI Agents to Autonomous Intelligence Systems uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. Defining AGEINT connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Defining AGEINT: From AI Agents to Autonomous Intelligence Systems rests on [299, 2026], [306, 2026], and [312, 2026]. Its anchor reference records: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for fixing what **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Defining AGEINT** in the evidence the row cites. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Defining AGEINT**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Defining AGEINT**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Defining AGEINT** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Defining AGEINT**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Defining AGEINT** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

45.2.2.2 Lesson 2: From LLMs to Agents: The Cognitive Controller Stack

Concept. From LLMs to Agents: The Cognitive Controller Stack uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. Without explicit treatment of **From LLMs to Agents**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. From LLMs to Agents: The Cognitive Controller Stack rests on [137, 2026]. The most specific cited work observes: It proposes a unified taxonomy organizing agent systems into six components: perception, brain, planning, action, tool use, and collaboration. Use it for the claim that **From LLMs to Agents: The Cognitive Controller Stack** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **From LLMs to Agents**, reason from the sources cited in this row. [137, 2026] An arXiv paper surveying the shift from passive language models to Agentic AI, where large language models act as cognitive controllers that combine memory, tool use, and environmental feedback to pursue extended goals. It proposes a unified taxonomy organizing agent systems into six components: perception, brain, planning, action, tool use, and collaboration. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **From LLMs to Agents**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **LLMs to Agents**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **From LLMs to Agents** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **From LLMs to Agents**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **From LLMs to Agents** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

45.2.2.3 Lesson 3: Unified Taxonomy: Perception → Brain → Planning → Action → Collaboration

Concept. Unified Taxonomy: Perception → Brain → Planning → Action → Collaboration connects cognitive science claims to analytic bias literacy: what the brain prioritizes, what it misses, and how review compensates.

Why it matters. Analysts use **Unified Taxonomy** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that treating pattern names as deployment playbooks would otherwise hide, and the reviewer accountable for challenge.

Source support. Unified Taxonomy: Perception → Brain → Planning → Action → Collaboration rests on [137, 2026]. The most specific cited work observes: It proposes a unified taxonomy organizing agent systems into six components: perception, brain, planning, action, tool use, and collaboration. Use it for fixing what **Unified Taxonomy: Perception → Brain → Planning → Action → Collaboration** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Unified Taxonomy**, work from the cited evidence behind this row. [137, 2026] An arXiv paper surveying the shift from passive language models to Agentic AI, where large language models act as cognitive controllers that combine memory, tool use, and environmental feedback to pursue extended goals. It proposes a unified taxonomy organizing agent systems into six components: perception, brain, planning, action, tool use, and collaboration. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Unified Taxonomy**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Unified Taxonomy**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Unified Taxonomy** work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Unified Taxonomy**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Unified Taxonomy** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

45.2.2.4 Lesson 4: Perception Modules: Multimodal Ingestion (Text, Vision, Audio, Sensor)

Concept. Perception Modules: Multimodal Ingestion (Text, Vision, Audio, Sensor) connects cognitive science claims to analytic bias literacy: what the brain prioritizes, what it misses, and how review compensates.

Why it matters. Perception Modules matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; treating pattern names as deployment playbooks is a common failure.

Source support. Perception Modules: Multimodal Ingestion (Text, Vision, Audio, Sensor) rests on [299, 2026], [306, 2026], and [312, 2026]. The closest source to this row notes: It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). Use them for the claim that **Perception Modules: Multimodal Ingestion (Text, Vision, Audio, Sensor)** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **Perception Modules** against the works cited for this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Perception Modules**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Perception Modules**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Perception Modules** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Perception Modules**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Perception Modules** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

45.2.2.5 Lesson 5: Brain/Reasoning: LLM as Cognitive Controller

Concept. Brain/Reasoning: LLM as Cognitive Controller connects cognitive science claims to analytic bias literacy: what the brain prioritizes, what it misses, and how review compensates.

Why it matters. Brain/Reasoning connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Brain/Reasoning: LLM as Cognitive Controller rests on [138, 2026]. The most specific cited work observes: It proposes a unified taxonomy decomposing LLM-based agents into six dimensions: core components, cognitive architecture, learning paradigms, multi-agent systems, environments and domains, and evaluation and safety. Use it for fixing what **Brain/Reasoning: LLM as Cognitive Controller** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Brain/Reasoning**, reason from the sources cited in this row. [138, 2026] An arXiv survey paper on agentic AI examining the shift from generative systems to autonomous agents that perceive, reason, plan, and act. It proposes a unified taxonomy decomposing LLM-based agents into six dimensions: core components, cognitive architecture, learning paradigms, multi-agent systems, environments and domains, and evaluation and safety. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Brain/Reasoning**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Brain/Reasoning**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Brain/Reasoning** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Brain/Reasoning**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Brain/Reasoning** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

45.2.2.6 Lesson 6: Memory: In-Context, External VectorDB, Episodic, Semantic, Procedural

Concept. Memory: In-Context, External VectorDB, Episodic, Semantic, Procedural treats agent memory terms as a pedagogical taxonomy unless a domain memory source is cited; MCP and official agentic-AI guidance support external-memory governance, tool boundaries, logs, retention, and reviewer control.

Why it matters. Memory: In-Context, External VectorDB, Episodic, Semantic, Procedural matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; treating pattern names as deployment playbooks is a common failure.

Source support. Memory: In-Context, External VectorDB, Episodic, Semantic, Procedural rests on [299, 2026], [306, 2026], and [312, 2026]. Its anchor reference records: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for the claim that **Memory: In-Context, External VectorDB, Episodic, Semantic, Procedural** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Memory: In-Context, External VectorDB, Episodic, Semantic, Procedural** in the evidence the row cites. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to

external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Memory**, build an agent-memory boundary card that separates source/change ledgers, external stores, retention rules, and reviewer controls from unsupported cognitive-memory taxonomy claims. Shape **Memory: In-Context, External VectorDB, Episodic, Semantic, Procedural** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Memory: In-Context, External VectorDB, Episodic, Semantic, Procedural**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Memory: In-Context, External VectorDB, Episodic, Semantic, Procedural** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

45.2.2.7 Lesson 7: Agentic cyber-misuse control review using sample prompt records, fabricated logs, and deny-by-default tool policies

Concept. Agentic cyber-misuse control review using sample prompt records, fabricated logs, and deny-by-default tool policies treats the topic as a misuse-case control problem: identify the agent permission, prompt path, tool boundary, and blocked outcome.

Why it matters. Agentic cyber-misuse control review matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; treating misuse taxonomy as tool permission is a common failure.

Source support. Agentic cyber-misuse control review using sample prompt records, fabricated logs, and deny-by-default tool policies rests on [299, 2026], [306, 2026], and [312, 2026]. The closest source to this row notes: It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). Use them for the claim that **Agentic cyber-misuse control review using sample prompt records, fabricated logs, and deny-by-default tool policies** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Agentic cyber-misuse control review**, reason from the sources cited in this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Agentic cyber-misuse control review**, build a blocked-request control card with tool permission, unsafe outcome, deny rule, log evidence, and reviewer disposition. Shape **Agentic cyber-misuse control review** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Agentic cyber-misuse control review**: that a misuse taxonomy describing what an autonomous agent could do is permission or a recipe to make it do so.

Transfer task. Reuse the **Agentic cyber-misuse control review** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

45.2.2.8 Lesson 8: Collaboration: A2A Messaging, Shared Context, Role Specialization

Concept. Collaboration: A2A Messaging, Shared Context, Role Specialization uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. Collaboration: A2A Messaging, Shared Context, Role Specialization matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; treating pattern names as deployment playbooks is a common failure.

Source support. Collaboration: A2A Messaging, Shared Context, Role Specialization rests on [139, 2026]. The most specific cited work observes: A LinkedIn post by Aishwarya Srinivasan discussing agentic AI design patterns for building production-grade AI agents. Use it for pinning down the scope of **Collaboration: A2A Messaging, Shared Context, Role Specialization**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Collaboration: A2A Messaging, Shared Context, Role Specialization** in the evidence the row cites. [139, 2026] A LinkedIn post by Aishwarya Srinivasan discussing agentic AI design patterns for building production-grade AI agents. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Collaboration**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Collaboration**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Collaboration: A2A Messaging, Shared Context, Role Specialization** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Collaboration: A2A Messaging, Shared Context, Role Specialization**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Collaboration: A2A Messaging, Shared Context, Role Specialization** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

45.2.2.9 Lesson 9: The OECD Agentic AI Landscape and Conceptual Foundations (2026)

Concept. The OECD Agentic AI Landscape and Conceptual Foundations (2026) evaluates agentic-AI governance claims against OECD principles: transparency, accountability, and human oversight.

Why it matters. The OECD Agentic AI Landscape connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. The OECD Agentic AI Landscape and Conceptual Foundations (2026) rests on [140, 2026]. Its anchor reference records: 56, February 2026) titled "The Agentic AI Landscape and Its Conceptual Foundations," prepared by OECD staff with an expert group. Use it for the claim that **The OECD Agentic AI Landscape and Conceptual Foundations (2026)** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **The OECD Agentic AI Landscape** in the evidence the row cites. [140, 2026] An OECD Artificial Intelligence Paper (No. 56, February 2026) titled "The Agentic AI Landscape and Its Conceptual Foundations," prepared by OECD staff with an expert group. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **The OECD Agentic AI Landscape**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **OECD Agentic AI Landscape and**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the

reviewer accountable for challenge. Shape **The OECD Agentic AI Landscape** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **The OECD Agentic AI Landscape**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **The OECD Agentic AI Landscape** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

45.2.2.10 Lesson 10: MIT Sloan Explanation of Agentic AI

Concept. MIT Sloan Explanation of Agentic AI evaluates agentic-AI governance claims against OECD principles: transparency, accountability, and human oversight.

Why it matters. MIT Sloan Explanation connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. MIT Sloan Explanation of Agentic AI rests on [141, 2026]. The most specific cited work observes: An MIT Sloan explainer article on agentic AI, defining autonomous software systems that perceive, reason, and act to complete multi-step tasks with minimal human intervention. Use it for pinning down the scope of **MIT Sloan Explanation of Agentic AI**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **MIT Sloan Explanation**, reason from the sources cited in this row. [141, 2026] An MIT Sloan explainer article on agentic AI, defining autonomous software systems that perceive, reason, and act to complete multi-step tasks with minimal human intervention. It distinguishes such agents from chatbots, cites a 2025 MIT Sloan/BCG survey finding 35% of companies had deployed agents with 44% planning to, and reviews business applications such as fraud detection and customer service. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **MIT Sloan Explanation**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **MIT Sloan Explanation of Agentic**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **MIT Sloan Explanation** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **MIT Sloan Explanation**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **MIT Sloan Explanation** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

45.2.2.11 Lesson 11: AGEINT vs. Traditional OSINT vs. AI-Assisted Analysis: A Capability Matrix

Concept. AGEINT vs. Traditional OSINT vs. AI-Assisted Analysis: A Capability Matrix treats open sources as publicly available evidence that still requires provenance, corroboration, legality, and minimization before reuse.

Why it matters. AGEINT vs. Traditional OSINT vs. AI-Assisted Analysis matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; treating pattern names as deployment playbooks is a common failure.

Source support. AGEINT vs. Traditional OSINT vs. AI-Assisted Analysis: A Capability Matrix rests on [301, 2026] and [298, 2026]. Its anchor reference records: Official Intelligence Community strategy for open-source intelligence governance, integration, source discovery, data, tools, tradecraft, and workforce priorities. Use them for fixing what **AGEINT vs. Traditional OSINT vs. AI-Assisted Analysis: A Capability Matrix** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **AGEINT vs. Traditional OSINT vs. AI-Assisted Analysis** against the works cited for this row. [301, 2026] Official Intelligence Community strategy for open-source intelligence governance, integration, source discovery, data, tools, tradecraft, and workforce priorities. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **AGEINT vs. Traditional OSINT vs. AI-Assisted Analysis**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **AGEINT vs Traditional OSINT vs**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **AGEINT vs. Traditional OSINT vs. AI-Assisted Analysis** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **AGEINT vs. Traditional OSINT vs. AI-Assisted Analysis**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **AGEINT vs. Traditional OSINT vs. AI-Assisted Analysis** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

45.2.2.12 Lesson 12: Dual-Paradigm Framework: Symbolic/Classical vs. Neural/Generative Agents

Concept. Dual-Paradigm Framework: Symbolic/Classical vs. Neural/Generative Agents uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. Dual-Paradigm Framework connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Dual-Paradigm Framework: Symbolic/Classical vs. Neural/Generative Agents rests on [142, 2026]. The lead source's own note reads: The arXiv abstract page for "Agentic AI: A Comprehensive Survey of Architectures, Applications," a 2025 paper by Mohamad Abou Ali and Fadi Dornaika. Use it for pinning down the scope of **Dual-Paradigm Framework: Symbolic/Classical vs. Neural/Generative Agents**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Dual-Paradigm Framework**, work from the cited evidence behind this row. [142, 2026] The arXiv abstract page for "Agentic AI: A Comprehensive Survey of Architectures, Applications," a 2025 paper by Mohamad Abou Ali and Fadi Dornaika. Based on a PRISMA systematic review of roughly 90 studies from 2018 to 2025, it proposes a dual-paradigm framework distinguishing symbolic/classical systems based on algorithmic planning and persistent state from neural/generative systems driven by stochastic generation and prompt orchestration. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Dual-Paradigm Framework**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Dual-Paradigm Framework**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Dual-Paradigm Framework** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Dual-Paradigm Framework**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Dual-Paradigm Framework** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

45.2.2.13 Lesson 13: The Return to HUMINT as Agentic AI Degrades Digital Trust Concept. The Return to HUMINT as Agentic AI Degrades Digital Trust

The Return to HUMINT as Agentic AI Degrades Digital Trust treats human-source work as a governed relationship: validation, consent, reporting, source protection, and oversight—not contact activity.

Why it matters. Without explicit treatment of **The Return to HUMINT as Agentic AI Degrades Digital Trust**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. The Return to HUMINT as Agentic AI Degrades Digital Trust rests on [004, 2026] and [005, 2026]. The closest source to this row notes: 70, No. Use them for the working definition that **The Return to HUMINT as Agentic AI Degrades Digital Trust** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **The Return to HUMINT as Agentic AI Degrades Digital Trust** against the works cited for this row. [004, 2026] Tom Mulligan argues that artificial intelligence will enhance rather than replace human intelligence professionals, contending that the future of intelligence lies in human-machine collaboration. He maintains that uniquely human qualities such as intuition, experience, and independent judgment become more valuable as adversaries gain access to the same AI tools. [005, 2026] A blog post on SemperVerus summarizing a CIA Studies in Intelligence article, "Espionage in Our AI Future: Why Human Intelligence Still Matters" (Vol. 70, No. 1, March 2026). It argues that as AI makes technical intelligence cheaper and AI-driven fabrication more pervasive, human intelligence becomes relatively more valuable, since human specialists are needed to verify source reliability over time. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **The Return to HUMINT as Agentic AI Degrades Digital Trust**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Return to HUMINT as Agentic**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape this subject work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **The Return to HUMINT as Agentic AI Degrades Digital Trust**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **The Return to HUMINT as Agentic AI Degrades Digital Trust** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

45.2.3 Foundations of AGEINT worked safe example: synthetic inputs, evidence, and review

Worked example: a synthetic research assistant agent organizes public readings for an instructor. [232, 2026]; [235, 2026].

Triangulation anchors. In module 31's worked-example section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **governed agentic intelligence**. Learners use a **agent run and assurance card** and keep this boundary visible: No autonomous external action, credentialed operations, live-target workflows, or uncontrolled tool use.

Frame. The classroom question centers on **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems**. Excluded actions stay explicit, and the **Agentic Tool-Governance Lens** planning question is: Which human authority, agent identity, tool permission, autonomy limit, incident threshold, and recoverability condition bounds the workflow?

Inputs. For the **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems** scenario, use public URLs, a fixed retrieval tool, a summarization prompt, a time budget, and a stop condition. The Agentic Tool-Governance Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems**, students bind the agent identity, list allowed tools, set autonomy limits, capture sources, block unsafe requests, and log approvals. Pause whenever an inference about Defining AGEINT: From AI Agents to Autonomous Intelligence Systems appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems** classroom scenario; unit artifact = agent run and assurance card; evidence = allowed inputs; method = least-privilege agent design and run review; output = an agent run card with tool calls, source links, blocked actions, reviewer notes, incident threshold, and recovery decision; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems** as "Agentic Tool-Governance Lens confirms it" is not enough. The revision ties the claim to least-privilege agent design and run review, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

45.2.4 Foundations of AGEINT practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Agentic Tool-Governance Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**.

Triangulation anchors. In module 31's practice-sequence section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Defining AGEINT: From AI Agents to Autonomous Intelligence Systems, From LLMs to Agents: The Cognitive Controller Stack, Unified Taxonomy: Perception → Brain → Planning → Action → Collaboration; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Agentic AI Governance and Tool Security** lane.

Move	Learner action	Output	Check
2. Frame	Answer the lens question: Which human authority, agent identity, tool permission, autonomy limit, incident threshold, and recoverability condition bounds the workflow?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Defining AGEINT: From AI Agents to Autonomous Intelligence Systems: agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the agent run and assurance card fields for Defining AGEINT: From AI Agents to Autonomous Intelligence Systems.	Unit profile note.	Evidence artifacts include tool-allowlist record, external-memory governance boundary.
4. Challenge	Test the misconception that naming an agent pattern certifies it is safe to deploy without governance gates.	Failure-mode note.	The artifact applies the key distinction: separate agent assistance from autonomous external action.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

45.2.4.1 Foundations of AGEINT instructor notes: source reasoning, review points, and studio focus Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**. [232, 2026]; [235, 2026].

45.2.4.2 Foundations of AGEINT extension exercise: peer validation and refresh trigger review **Evidence anchor.** Section 45; [232, 2026].
Have learners swap artifacts and apply the **Agentic Tool-Governance Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**.

45.2.5 Foundations of AGEINT knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 45; [232, 2026].

1. Explain how **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems** is defined here; name the source descriptor that supports the definition.
2. Contrast **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems** with **From LLMs to Agents: The Cognitive Controller Stack** using the **Agentic Tool-Governance Lens** artifact fields.
3. Identify one failure mode from the **Agentic AI Governance and Tool Security** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which permission can be removed while preserving the learning objective?
5. Correct this misconception: that naming an agent pattern certifies it is safe to deploy without governance gates.

45.2.5.1 Foundations of AGEINT answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems** without source evidence, uncertainty, or a safe transfer task.

45.3 Foundations of AGEINT assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 45; [232, 2026].

45.3.1 Foundations of AGEINT evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 45; [232, 2026].

45.3.2 Foundations of AGEINT transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 45; [232, 2026].

45.3.2.1 Foundations of AGEINT lineage and source tradition: profile, concepts, and first anchors This sits in the **Agentic AI Governance and Tool Security** lineage: delegated action under explicit authority, identity, permissions, tool boundaries, monitoring, and human escalation. [232, 2026]; [235, 2026].

45.3.2.2 Foundations of AGEINT working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 45; [232, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**, with provenance and reviewability throughout.

45.3.2.3 Foundations of AGEINT knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [232, 2026]; [235, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

45.3.2.4 Foundations of AGEINT transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 45; [232, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**.
- **Evidence contract:** keep the **Agentic AI Governance and Tool Security** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

45.3.2.5 Foundations of AGEINT profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 45; [232, 2026].

The matched profile emphasizes delegated action under explicit authority, identity, permissions, tool boundaries, monitoring, and human escalation. The method stack is AI RMF Govern-Map-Measure-Manage, least-privilege tool design, prompt-injection review, progressive deployment, and rollback drills; the local topic cluster is **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**.

45.3.3 Foundations of AGEINT evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 45; [232, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Agentic AI Governance and Tool Security** profile tells reviewers what evidence is strong enough for the module artifact built around **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**.

45.3.3.1 Foundations of AGEINT guide source spine: inherited keys and local citation roles Primary guide citations: [232, 2026]; [235, 2026]; [247, 2026]; [279, 2026]; [282, 2026]; [284, 2026]; [289, 2026]; [291, 2026]; [296, 2026]; [137, 2026]; [138, 2026]; [139, 2026]; [140, 2026]; [141, 2026]; [142, 2026]; [004, 2026]; [005, 2026]; [299, 2026]; [306, 2026]; [312, 2026]; [301, 2026]; [298, 2026].

45.3.3.2 Foundations of AGEINT verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [232, 2026]; [235, 2026].

Tier	What counts	How it is used
Source guide	[232, 2026]; [235, 2026]; [247, 2026]; [279, 2026]; [282, 2026]; [284, 2026]; [289, 2026]; [291, 2026]; [296, 2026]; [137, 2026]; [138, 2026]; [139, 2026]; [140, 2026]; [141, 2026]; [142, 2026]; [004, 2026]; [005, 2026]; [299, 2026]; [306, 2026]; [312, 2026]; [301, 2026]; [298, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 31's source-canon section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack** and [232, 2026]; [235, 2026], but only directly verified source URLs are encoded as citations.

45.3.3.3 Foundations of AGEINT intelligence practice lens: evidence artifact and safety check Practice lens: **Agentic Tool-Governance Lens** for **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**. [232, 2026]; [235, 2026].

Planning question: Which human authority, agent identity, tool permission, autonomy limit, incident threshold, and recoverability condition bounds the workflow?

Evidence artifact: agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path.

Validation rule: verify least privilege, prompt-injection exposure, provenance, observability, stop conditions, and incident-reporting triggers. Applied to **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**.

Handoff contract: export agent traces, tool calls, retrieved sources, policy decisions, and human approvals separately.

Safety check: block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions.

45.3.3.4 Foundations of AGEINT runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 45; [232, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	31.99	31.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Foundations of AGEINT to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
AGEINT pattern registry, agent identity, and interface-contract studio	31.100	31.100 source title transformed into safe curriculum treatment; original: V2 AGEINT-depth extension: add agent evaluation and public-sector adoption gates that bind agency authority, AI Office-style accountability, impact assessment, and human review before any classroom agent workflow is rehearsed	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Bounded autonomy, procurement, incident-response, and assurance studio	31.101	31.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Foundations of AGEINT	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Model-card, recoverability, retention, and learner-support evidence package	31.102	31.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Foundations of AGEINT	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Defining AGEINT: From AI Agents to Autonomous Intelligence Systems	31.1	31.1 Defining AGEINT: From AI Agents to Autonomous Intelligence Systems	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
From LLMs to Agents: The Cognitive Controller Stack	31.2	31.2 From LLMs to Agents: The Cognitive Controller Stack	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Unified Taxonomy: Perception → Brain → Planning → Action → Collaboration	31.3	31.3 Unified Taxonomy: Perception → Brain → Planning → Action → Collaboration	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Perception Modules: Multimodal Ingestion (Text, Vision, Audio, Sensor)	31.3.1	31.3.1 Perception Modules: Multimodal Ingestion (Text, Vision, Audio, Sensor)	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Brain/Reasoning: LLM as Cognitive Controller	31.3.2	31.3.2 Brain/Reasoning: LLM as Cognitive Controller	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Memory: In-Context, External VectorDB, Episodic, Semantic, Procedural	31.3.3	31.3.3 Memory: In-Context, External VectorDB, Episodic, Semantic, Procedural	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Agentic cyber-misuse control review using sample prompt records, fabricated logs, and deny-by-default tool policies	31.3.4	31.3.4 source title transformed into safe curriculum treatment; original: Action: Tool Use, API Calls, Code Execution, Computer Use	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Collaboration: A2A Messaging, Shared Context, Role Specialization	31.3.5	31.3.5 Collaboration: A2A Messaging, Shared Context, Role Specialization	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
The OECD Agentic AI Landscape and Conceptual Foundations (2026)	31.4	31.4 The OECD Agentic AI Landscape and Conceptual Foundations (2026)	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
MIT Sloan Explanation of Agentic AI	31.5	31.5 MIT Sloan Explanation of Agentic AI	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
AGEINT vs. Traditional OSINT vs. AI-Assisted Analysis: A Capability Matrix	31.6	31.6 AGEINT vs. Traditional OSINT vs. AI-Assisted Analysis: A Capability Matrix	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Dual-Paradigm Framework: Symbolic/Classical vs. Neural/Generative Agents	31.7	31.7 Dual-Paradigm Framework: Symbolic/Classical vs. Neural/Generative Agents	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
The Return to HUMINT as Agentic AI Degrades Digital Trust	31.8	31.8 The Return to HUMINT as Agentic AI Degrades Digital Trust	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

45.3.3.5 Foundations of AGEINT reusable subsection contract: topic rows, artifacts, and safety duties **Evidence anchor.** Section 45; [232, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Defining AGEINT: From AI Agents to Autonomous Intelligence Systems	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
From LLMs to Agents: The Cognitive Controller Stack	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Unified Taxonomy: Perception → Brain → Planning → Action → Collaboration	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Perception Modules: Multimodal Ingestion (Text, Vision, Audio, Sensor)	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Brain/Reasoning: LLM as Cognitive Controller	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Memory: In-Context, External VectorDB, Episodic, Semantic, Procedural	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Agentic cyber-misuse control review using sample prompt records, fabricated logs, and deny-by-default tool policies	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Collaboration: A2A Messaging, Shared Context, Role Specialization	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
The OECD Agentic AI Landscape and Conceptual Foundations (2026)	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
MIT Sloan Explanation of Agentic AI	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
AGEINT vs. Traditional OSINT vs. AI-Assisted Analysis: A Capability Matrix	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Dual-Paradigm Framework: Symbolic/Classical vs. Neural/Generative Agents	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
The Return to HUMINT as Agentic AI Degrades Digital Trust	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

45.3.3.6 Foundations of AGEINT annotated source ledger: real titles and local contribution Each source cited by this **Agentic AI Governance and Tool Security** module is paired below with its real title and a one-line note on what it contributes to **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**.

Source	Cited work	What it contributes	Status
[232, 2026]	European AI Office	The European AI Office is the European Commission's central hub for developing and implementing AI governance across the EU, established to support trustworthy AI adoption while protecting people from associated risks. Its responsibilities include enforcing regulations for general-purpose AI models, implementing the AI Act, developing evaluation tools and benchmarks for assessing AI capabilities, and investigating potential regulatory violations.	verified source-guide
[235, 2026]	ISO/IEC 42005:2025 AI System Impact Assessment	ISO standard page for AI system impact assessment.	original source-guide
[247, 2026]	AI in the Public Sector	Official OECD.AI public-sector AI theme page.	original source-guide
[279, 2026]	Open Contracting Data Standard	The documentation homepage for the Open Contracting Data Standard, version 1.1.5, maintained by the Open Contracting Partnership to support disclosure of government contracting data across the procurement lifecycle. It provides a common data model spanning planning, tender, award, contract, and implementation stages, along with a primer, implementation guidance, technical schemas, and validation tooling.	verified source-guide
[282, 2026]	AI Research: Security and Resilience	A NIST page on AI research focused on security and resilience, framing these as core characteristics of trustworthy AI under the NIST AI Risk Management Framework.	verified source-guide
[284, 2026]	Verifiable Credential Data Integrity 1.0	The W3C Recommendation for Verifiable Credential Data Integrity 1.0, published May 2025, defining mechanisms for ensuring the authenticity and integrity of verifiable credentials using cryptographic proofs. It specifies a process of data transformation, hashing, and proof generation, and a corresponding verification procedure, along with a proof data model containing properties such as type, verification method, purpose, and proof value.	verified source-guide
[289, 2026]	Guidance for Organisations Using the Algorithmic Transparency Recording Standard	This is a GOV.UK guidance page published by the Government Digital Service that instructs public sector organizations on completing the Algorithmic Transparency Recording Standard (ATRS) template and publishing their records to the GOV.UK repository. It applies both to central government bodies required to publish under mandatory policy and to other public sector bodies doing so voluntarily.	verified source-guide
[291, 2026]	Revised 508 Standards and 255 Guidelines	Official documentation from the U.S. Access Board on the Revised 508 Standards and 255 Guidelines for information and communication technology accessibility. It establishes mandatory accessibility requirements for federal agencies and voluntary guidelines for telecommunications manufacturers, covering hardware, software, websites, electronic documents, and support services.	verified source-guide

Source	Cited work	What it contributes	Status
[296, 2026]	Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile	NIST AI 600-1, the Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, a cross-sectoral companion resource to the NIST AI RMF 1.0 issued pursuant to Executive Order 14110. It identifies risks that are unique to or amplified by generative AI and organizes suggested actions for managing those risks, mapped to the AI RMF functions.	verified source-guide
[137, 2026]	[2601.12560] Agentic Artificial Intelligence (AI)	An arXiv paper surveying the shift from passive language models to Agentic AI, where large language models act as cognitive controllers that combine memory, tool use, and environmental feedback to pursue extended goals. It proposes a unified taxonomy organizing agent systems into six components: perception, brain, planning, action, tool use, and collaboration.	verified source-guide
[138, 2026]	Agentic Artificial Intelligence (AI): Architectures, Taxonomies	An arXiv survey paper on agentic AI examining the shift from generative systems to autonomous agents that perceive, reason, plan, and act. It proposes a unified taxonomy decomposing LLM-based agents into six dimensions: core components, cognitive architecture, learning paradigms, multi-agent systems, environments and domains, and evaluation and safety.	verified source-guide
[139, 2026]	Agentic AI Design Patterns by Andrew Ng	A LinkedIn post by Aishwarya Srinivasan discussing agentic AI design patterns for building production-grade AI agents.	verified practitioner context; secondary evidence only
[140, 2026]	The agentic AI landscape and its conceptual foundations	An OECD Artificial Intelligence Paper (No. 56, February 2026) titled “The Agentic AI Landscape and Its Conceptual Foundations,” prepared by OECD staff with an expert group.	verified source-guide
[141, 2026]	Agentic AI, explained	An MIT Sloan explainer article on agentic AI, defining autonomous software systems that perceive, reason, and act to complete multi-step tasks with minimal human intervention. It distinguishes such agents from chatbots, cites a 2025 MIT Sloan/BCG survey finding 35% of companies had deployed agents with 44% planning to, and reviews business applications such as fraud detection and customer service.	verified practitioner context; secondary evidence only
[142, 2026]	Agentic AI: A Comprehensive Survey of Architectures, Applications	The arXiv abstract page for “Agentic AI: A Comprehensive Survey of Architectures, Applications,” a 2025 paper by Mohamad Abou Ali and Fadi Dornaika. Based on a PRISMA systematic review of roughly 90 studies from 2018 to 2025, it proposes a dual-paradigm framework distinguishing symbolic/classical systems based on algorithmic planning and persistent state from neural/generative systems driven by stochastic generation and prompt orchestration.	verified source-guide

Source	Cited work	What it contributes	Status
[004, 2026]	AI Won't Replace Spies—It Will Make Them More Powerful Than Ever	Tom Mulligan argues that artificial intelligence will enhance rather than replace human intelligence professionals, contending that the future of intelligence lies in human-machine collaboration. He maintains that uniquely human qualities such as intuition, experience, and independent judgment become more valuable as adversaries gain access to the same AI tools.	verified source-guide
[005, 2026]	CIA: Studies in AI and Human Intelligence - SemperVerus	A blog post on SemperVerus summarizing a CIA Studies in Intelligence article, "Espionage in Our AI Future: Why Human Intelligence Still Matters" (Vol. 70, No. 1, March 2026). It argues that as AI makes technical intelligence cheaper and AI-driven fabrication more pervasive, human intelligence becomes relatively more valuable, since human specialists are needed to verify source reliability over time.	verified source-guide
[299, 2026]	Model Context Protocol Specification	The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation).	verified source-guide context; use pinned MCP anchor for normative claims
[306, 2026]	Artificial Intelligence	Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support.	original source-guide
[312, 2026]	Guide on the Use of Agentic Artificial Intelligence	Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support.	original source-guide
[301, 2026]	The IC OSINT Strategy 2024-2026	Official Intelligence Community strategy for open-source intelligence governance, integration, source discovery, data, tools, tradecraft, and workforce priorities.	original source-guide
[298, 2026]	Intelligence Community Directives	Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations.	original source-guide

Where this sits. This module's overview is Section 45; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

45.3.4 Foundations of AGEINT governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 45; [232, 2026].

45.3.5 Foundations of AGEINT analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 31's governance-boundary section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Research lane: **Agentic AI Governance and Tool Security** for **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**. [232, 2026]; [235, 2026].
Curriculum topic spine: Defining AGEINT: From AI Agents to Autonomous Intelligence Systems, **From LLMs to Agents: The Cognitive Controller Stack**, **Unified Taxonomy: Perception → Brain → Planning → Action → Collaboration**. **Verified anchor cluster:** [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]; [Community, 2020b]; [Community, 2020a]; [of the Director of National Intelligence, 2025b].
Conceptual depth: delegated action under explicit authority, identity, permissions, tool boundaries, monitoring, and human escalation.
Method stack: AI RMF Govern-Map-Measure-Manage, least-privilege tool design, prompt-injection review, progressive deployment, and rollback drills.
Composability contract: agents, tools, credentials, memory, retrieval stores, policies, and logs remain separately inspectable and revocable components.
Known failure modes: excessive agency, shadow tools, indirect prompt injection, memory poisoning, confused authority, and unbounded action chains.
Defensive boundary: agentic workflows stay synthetic, owned-lab, supervised, logged, rate-limited, and reversible unless a lawful production authority exists. Applied to **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**.

Anchor	Why it matters here
[OECD, 2026a]	Official OECD conceptual foundation for agentic AI. Checked as of 2026-05-21; role: source_quality_anchor.
[of Canada Secretariat, 2026a]	Government of Canada guide for accountable public-sector use of agentic AI, including governance, risk, transparency, testing, monitoring, and human oversight considerations. Checked as of 2026-05-24; role: curriculum_anchor.
[of Standards and Technology, 2023]	Official NIST.AI.100-1 risk-management framework. Checked as of 2026-05-21; role: source_quality_anchor.
[of Standards and Technology, 2024d]	Official NIST AI 600-1 generative AI profile. Checked as of 2026-05-21; role: source_quality_anchor.
[Community, 2020b]	Official IC principles for lawful, accountable, objective, human-centered, secure, resilient, and science-informed AI. Checked as of 2026-05-21; role: curriculum_anchor.
[Community, 2020a]	Official IC framework for AI goals, authorities, human judgment, bias mitigation, testing, documentation, explainability, and review. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2025b]	Official IC AI governance directive covering CAIO roles, oversight, interoperability, civil-liberties review, training data, and impact assessment. Checked as of 2026-05-21; role: curriculum_anchor.

45.3.5.1 Foundations of AGEINT evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **Agentic AI Governance and Tool Security** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [232, 2026]; [235, 2026].

45.3.6 Foundations of AGEINT agentic boundary: assist, approve, block, and record

Evidence anchor. Section 45; [232, 2026].
AGEINT translation is bounded by the **Agentic AI Governance and Tool Security** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**.

45.3.6.1 Foundations of AGEINT permitted defensive utility: curriculum uses and safe outputs

Evidence anchor. Section 45; [232, 2026].
The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**.

45.3.6.2 Foundations of AGEINT excluded operational boundary: blocked actions and stop rules

Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [232, 2026]; [235, 2026] and **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

45.3.7 Foundations of AGEINT governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 45; [232, 2026].
Governance is practiced as a gate on the **Agentic AI Governance and Tool Security** lane. Learners use the **Agentic Tool-Governance Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**.

45.3.7.1 Foundations of AGEINT governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [232, 2026]; [235, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Agentic AI Governance and Tool Security** failure modes and the **Agentic Tool-Governance Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

45.3.7.2 Foundations of AGEINT evidence package handoff: appendices, records, and reuse

Evidence anchor. Section 45; [232, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Agentic Tool-Governance Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**.

45.3.7.3 Foundations of AGEINT current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**. [232, 2026]; [235, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_oecd_agentic_ai` for **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**?	The Agentic AI Landscape and Its Conceptual Foundations; lane `source_quality_spine`; checked 2026-05-21.	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path; Official OECD conceptual foundation for agentic AI.
What does the module inherit from `official_canada_agentic_ai_guide` for **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**?	Guide on the Use of Agentic Artificial Intelligence; lane `public_sector_agentic_ai`; checked 2026-05-24.	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path; bounded-autonomy run card, recoverability review, approval threshold, monitoring evidence, and public-sector service assurance
What does the module inherit from `official_nist_ai_rmf` for **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**?	Artificial Intelligence Risk Management Framework (AI RMF 1.0); lane `source_quality_spine`; checked 2026-05-21.	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path; Official NIST.AI.100-1 risk-management framework.
What does the module inherit from `official_nist_ai_600_1` for **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**?	Artificial Intelligence Risk Management Framework: Generative AI Profile; lane `source_quality_spine`; checked 2026-05-21.	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path; Official NIST AI 600-1 generative AI profile.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 45; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

45.3.8 Foundations of AGEINT assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 45; [232, 2026].

45.3.9 Foundations of AGEINT assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 45; [232, 2026].

45.3.9.1 Foundations of AGEINT capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack** and [232, 2026]; [235, 2026].

45.3.9.2 Foundations of AGEINT instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack** and [232, 2026]; [235, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

45.3.9.3 Foundations of AGEINT assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Defining AGEINT: From AI Agents to Autonomous Intelligence Systems	Completed **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
From LLMs to Agents: The Cognitive Controller Stack	Completed **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Unified Taxonomy: Perception → Brain → Planning → Action → Collaboration	Completed **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

45.3.10 Foundations of AGEINT refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [232, 2026]; [235, 2026] and **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**.

45.3.10.1 Foundations of AGEINT refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**. The local signals begin with [232, 2026]; [235, 2026].

45.3.10.2 Foundations of AGEINT claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**, and the source spine for these checks begins with [232, 2026]; [235, 2026].

45.3.11 Foundations of AGEINT reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [232, 2026]; [235, 2026].

Triangulation anchors. In module 31's review-checklist section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack**. [232, 2026]; [235, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

45.3.12 Foundations of AGEINT learning-path links: module map, overview, and curriculum atlas

Use the cross-links below to place **Defining AGEINT: From AI Agents to Autonomous Intelligence Systems; From LLMs to Agents: The Cognitive Controller Stack** in the wider unit: the orientation sets the frame, the parent unit supplies the shared safety posture, and the neighbouring modules show what evidence enters and leaves. Lead sources: [232, 2026]; [235, 2026].

Section 2, Section 44, Section 46

46 AGEINT Design Patterns and Archetypes

46.0.1 AGEINT Design Patterns and Archetypes figures and course links: visual evidence, source flow, and navigation

The module uses Figure 89, Figure 90, and Figure 85 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 44, Section 45, Section 47.
This module teaches the **Agentic AI Governance and Tool Security** lane through a bounded, source-backed coursebook chapter. [233, 2026]; [258, 2026].

46.1 Agentic AI Governance and Tool Security frame for AGEINT Design Patterns and Archetypes: source context, topic focus, and reader task

Evidence anchor. Section 46; [233, 2026].

46.1.1 AGEINT Design Patterns and Archetypes orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 46; [233, 2026].

46.1.2 AGEINT Design Patterns and Archetypes conceptual primer: source context, core model, and reader task

This chapter teaches agentic AI as delegated action under control: identity, authority, tool permissions, memory, logs, stop conditions, and recoverability define what an agent may do. The chapter uses **Agentic Tool-Governance Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**.
The central distinction is to separate agent assistance from autonomous external action. Core topics include **Pattern 1: Focused Analytic Reasoner (source identity preserved in pattern registry) - keeps reasoning reviewable without exposing hidden reasoning or delegating action; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes; Safe defensive application: single public-source report critique with provenance and uncertainty fields**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [233, 2026]; [258, 2026].
Learners move from vocabulary and the **Agentic Tool-Governance Lens** distinction through topic lessons on **Pattern 1: Focused Analytic Reasoner (source identity preserved in pattern registry) - keeps reasoning reviewable without exposing hidden reasoning or delegating action** with evidence and misconception checks, then assemble an **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** with safety and rights gates.

46.1.3 AGEINT Design Patterns and Archetypes learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 46; [233, 2026].

- Connect **Pattern 1: Focused Analytic Reasoner (source identity preserved in pattern registry) - keeps reasoning reviewable without exposing hidden reasoning or delegating action and Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes** to **Agentic AI Governance and Tool Security** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build an **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate agent assistance from autonomous external action; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as excessive agency, shadow tools, indirect prompt injection, memory poisoning, confused authority, and unbounded action chains, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: agentic workflows stay synthetic, owned-lab, supervised, logged, rate-limited, and reversible unless a lawful production authority exists.

46.1.4 AGEINT Design Patterns and Archetypes core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 46; [233, 2026].

Term	Working definition
Agent identity	the named software actor, role, and authorization context for a run
Tool allowlist	the bounded set of actions the agent may request
Delegation	the handoff of a task under explicit human authority and review
Bounded autonomy	the documented ceiling on what an agent may decide or request without review
Recoverability	the path back to a known-safe state after a bad output or action request
AI incident	a logged event where an AI system creates or plausibly creates harm or loss of control
Prompt injection	untrusted content that attempts to override instructions or authority boundaries
Pattern registry	the catalog of approved agent behaviors, prompts, and evaluation hooks
Adversarial eval	structured tests that probe agent misuse, injection, and over-delegation before release
Pattern 1: Focused Analytic Reasoner (source…	Key terms: Pattern, Focused, Analytic.
Safe methods: bounded source reading, explicit…	Key terms: methods, bounded, reading.

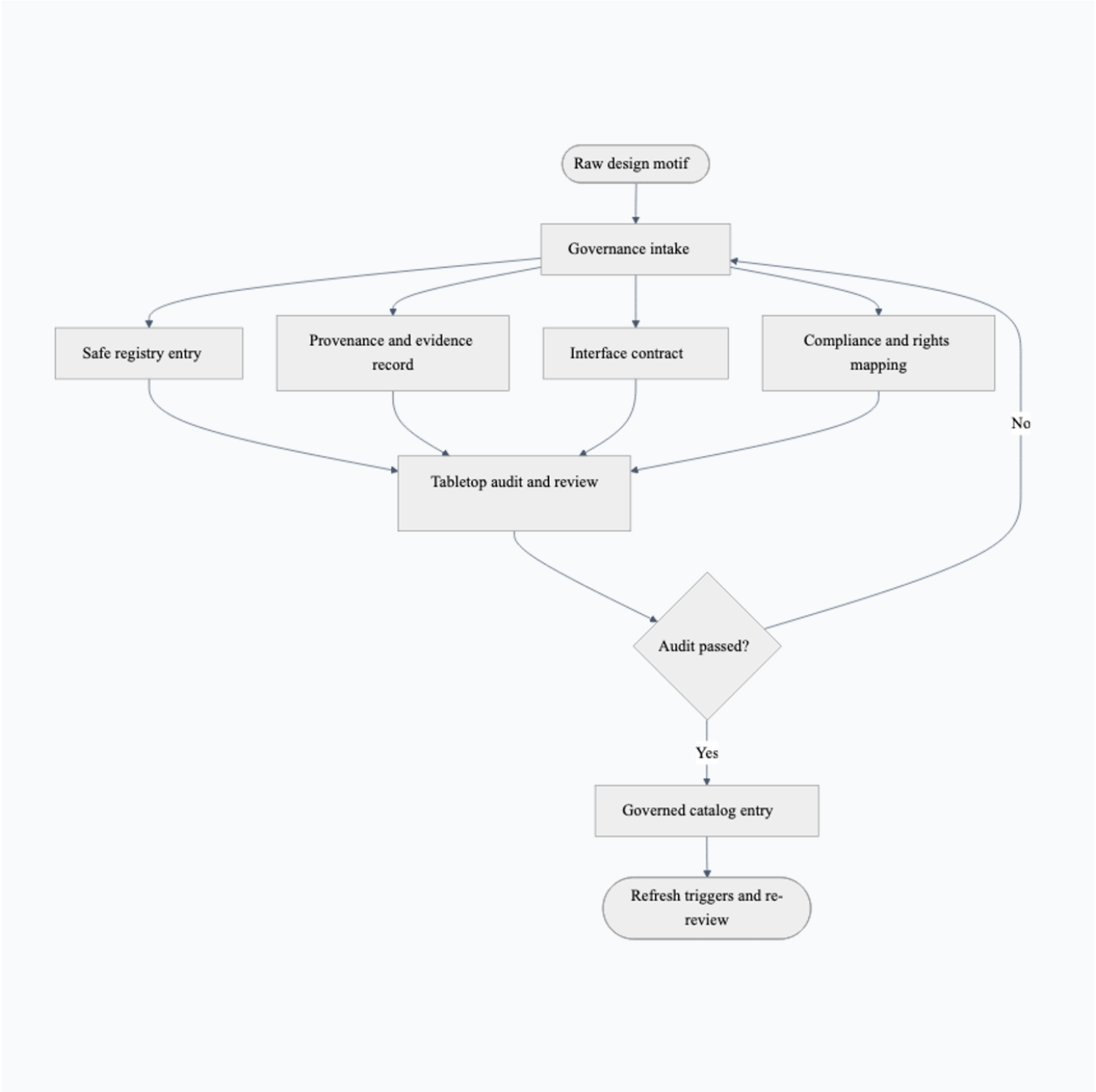


Figure 89: This diagram shows how each AGEINT design pattern is converted into a documented, auditable governance artifact rather than an operational deployment. In the ageint agentic intelligence / ageint design patterns and archetypes section, it lets readers compare A top-to-bottom transform. A raw design motif enters a governance intake. It splits into four parallel artifacts: a safe registry entry, a provenance, evidence record, and an interface contract so the visual functions as a traceable course aid rather than an unscoped assertion.

Figure 90: The pattern taxonomy groups AGEINT design patterns by safe curriculum role. The captioned view belongs to the ageint agentic intelligence / ageint design patterns and archetypes section and should be read as a map of pattern taxonomy categories, denominators, evidence lanes, limitations, and reviewer-use cautions, not as a capability score or live-task instruction.

46.2 Agentic Tool-Governance Lens path for AGEINT Design Patterns and Archetypes: lesson cluster, safe artifact, and review

Evidence anchor. Section 46; [233, 2026].

46.2.1 AGEINT Design Patterns and Archetypes practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 46; [233, 2026].

46.2.2 AGEINT Design Patterns and Archetypes topic lessons: source-backed concepts and transfer tasks

This module builds agentic AI as delegated action under control: identity, authority, tool permissions, memory, logs, stop conditions, and recoverability define what an agent may do. The sequence opens with **Pattern 1: Focused Analytic Reasoner (source identity preserved in pattern registry) - keeps reasoning reviewable without exposing hidden reasoning or delegating action**, **Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**, **Safe defensive application: single public-source report critique with provenance and uncertainty fields** and applies the **Agentic Tool-Governance Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 85; module overview Section 46; curriculum atlas Section 2.

Triangulation anchors. In module 32's topic-lessons section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

46.2.2.1 Lesson 1: Pattern 1: Focused Analytic Reasoner (source identity preserved in pattern registry) - keeps reasoning reviewable without exposing hidden reasoning or delegating action

Concept. Pattern 1: Focused Analytic Reasoner (source identity preserved in pattern registry) - keeps reasoning reviewable without exposing hidden reasoning or delegating action uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Analysts use **Pattern 1: Focused Analytic Reasoner (source identity preserved in pattern registry) - keeps reasoning reviewable without exposing hidden reasoning or delegating action** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that treating pattern names as deployment playbooks would otherwise hide, and the reviewer accountable for challenge.

Source support. Pattern 1: Focused Analytic Reasoner (source identity preserved in pattern registry) - keeps reasoning reviewable without exposing hidden reasoning or delegating action rests on [143, 2026]. The most specific cited work observes: A Medium article by Anil Jain (2025) surveying agentic AI system architectures and design patterns. Use it for the working definition that **Pattern 1: Focused Analytic Reasoner (source identity preserved in pattern registry) - keeps reasoning reviewable without exposing hidden reasoning or delegating action** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Pattern 1: Focused Analytic Reasoner (source identity preserved in pattern registry) - keeps reasoning reviewable without exposing hidden reasoning or delegating action**, reason from the sources cited in this row. [143, 2026] A Medium article by Anil Jain (2025) surveying agentic AI system architectures and design patterns. It defines agentic AI as systems capable of independent decision-making, reviews frameworks such as LangChain, LlamaIndex, and AutoGen, and describes five system components: perception, decision-making, action, memory, and communication. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Pattern 1**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Pattern 1**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Pattern 1: Focused Analytic Reasoner (source identity preserved in pattern registry) - keeps reasoning reviewable without exposing hidden reasoning or delegating action** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Pattern 1: Focused Analytic Reasoner (source identity preserved in pattern registry) - keeps reasoning reviewable without exposing hidden reasoning or delegating action** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.2 Lesson 2: Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes

Concept. Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. Safe methods connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes rests on [309, 2026], [310, 2026], and [300, 2026]. The most specific cited work observes: It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). Use them for the claim that **Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Safe methods** in the evidence the row cites. [309, 2026] An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection. [310, 2026] The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Safe methods**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe methods**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe methods** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Safe methods**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe methods** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.3 Lesson 3: Safe defensive application: single public-source report critique with provenance and uncertainty fields

Concept. Safe defensive application: single public-source report critique with provenance and uncertainty fields uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. Without explicit treatment of **Safe defensive application**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Safe defensive application: single public-source report critique with provenance and uncertainty fields rests on [309, 2026], [310, 2026], and [300, 2026]. The most specific cited work observes: It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). Use them for the claim that **Safe defensive application: single public-source report critique with provenance and uncertainty fields** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **Safe defensive application** against the works cited for this row. [309, 2026] An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection. [310, 2026] The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Safe defensive application**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe defensive application**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe defensive application** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Safe defensive application**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe defensive application** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.4 Lesson 4: Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Focused Analytic Reasoner

Concept. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Focused Analytic Reasoner uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Without explicit treatment of **Safe architecture artifact**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Focused Analytic Reasoner rests on [299, 2026], [306, 2026], and [312, 2026]. The lead source's own note reads: It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). Use them for the working definition that **Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Focused Analytic Reasoner** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **Safe architecture artifact** against the works cited for this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Safe architecture artifact**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe architecture artifact**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe architecture artifact** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Safe architecture artifact**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe architecture artifact** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.5 Lesson 5: Pattern 2: Reflection and Bias-Check Agent (source identity preserved in pattern registry) - supports quality review and never replaces accountable human judgment

Concept. Pattern 2: Reflection and Bias-Check Agent (source identity preserved in pattern registry) - supports quality review and never replaces accountable human judgment uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Pattern 2: Reflection and Bias-Check Agent (source identity preserved in pattern registry) - supports quality review and never replaces accountable human judgment matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; treating pattern names as deployment playbooks is a common failure.

Source support. Pattern 2: Reflection and Bias-Check Agent (source identity preserved in pattern registry) - supports quality review and never replaces accountable human judgment rests on [139, 2026]. The closest source to this row notes: A LinkedIn post by Aishwarya Srinivasan discussing agentic AI design patterns for building production-grade AI agents. Use it for the working definition that **Pattern 2: Reflection and Bias-Check Agent (source identity preserved in pattern registry) - supports quality review and never replaces accountable human judgment** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Pattern 2: Reflection and Bias-Check Agent (source identity preserved in pattern registry) - supports quality review and never replaces accountable human judgment**, reason from the sources cited in this row. [139, 2026] A LinkedIn post by Aishwarya Srinivasan discussing agentic AI design patterns for building production-grade AI agents. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Pattern 2**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Pattern**

2, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Pattern 2: Reflection and Bias-Check Agent (source identity preserved in pattern registry) - supports quality review and never replaces accountable human judgment** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Pattern 2: Reflection and Bias-Check Agent (source identity preserved in pattern registry) - supports quality review and never replaces accountable human judgment**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Pattern 2: Reflection and Bias-Check Agent (source identity preserved in pattern registry) - supports quality review and never replaces accountable human judgment** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.6 Lesson 6: Safe methods: rubric-based critique, source-quality scoring, and trajectory validation

Concept. Safe methods: rubric-based critique, source-quality scoring, and trajectory validation uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. Safe methods matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; treating pattern names as deployment playbooks is a common failure.

Source support. Safe methods: rubric-based critique, source-quality scoring, and trajectory validation rests on [306, 2026] and [312, 2026]. The lead source's own note reads: Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Use them for the working definition that **Safe methods: rubric-based critique, source-quality scoring, and trajectory validation** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **Safe methods** against the works cited for this row. [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Safe methods**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe methods**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe methods** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Safe methods**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe methods** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.7 Lesson 7: Safe defensive application: analytic-bias review over a synthetic or public-source evidence packet

Concept. Safe defensive application: analytic-bias review over a synthetic or public-source evidence packet treats open sources as publicly available evidence that still requires provenance, corroboration, legality, and minimization before reuse.

Why it matters. Analysts use **Safe defensive application** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that treating pattern names as deployment playbooks would otherwise hide, and the reviewer accountable for challenge.

Source support. Safe defensive application: analytic-bias review over a synthetic or public-source evidence packet rests on [297, 2026] and [298, 2026]. The most specific cited work observes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for the working definition that **Safe defensive application: analytic-bias review over a synthetic or public-source evidence packet** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Safe defensive application**, reason from the sources cited in this row. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Safe defensive application**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe defensive application**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe defensive application** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Safe defensive application**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe defensive application** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.8 Lesson 8: Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Reflection and Bias-Check Agent

Concept. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Reflection and Bias-Check Agent uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Safe architecture artifact connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Reflection and Bias-Check Agent rests on [299, 2026], [306, 2026], and [312, 2026]. The closest source to this row notes: It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). Use them for the working definition that **Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Reflection and Bias-Check Agent** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Safe architecture artifact**, reason from the sources cited in this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Safe architecture artifact**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe architecture artifact**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe architecture artifact** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Safe architecture artifact**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe architecture artifact** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.9 Lesson 9: Pattern 3: Tool-Allowlist Research Assistant (source identity preserved in pattern registry) - excludes broad scraping, credentialed collection, and exposure-search tooling

Concept. Pattern 3: Tool-Allowlist Research Assistant (source identity preserved in pattern registry) - excludes broad scraping, credentialed collection, and exposure-search tooling uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Pattern 3: Tool-Allowlist Research Assistant (source identity preserved in pattern registry) - excludes broad scraping, credentialed collection, and exposure-search tooling connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Pattern 3: Tool-Allowlist Research Assistant (source identity preserved in pattern registry) - excludes broad scraping, credentialed collection, and exposure-search tooling rests on [144, 2026]. The closest source to this row notes: An AWS Prescriptive Guidance document (July 2025) introducing agentic AI patterns and workflows. Use it for pinning down the scope of **Pattern 3: Tool-Allowlist Research Assistant (source identity preserved in pattern registry) - excludes broad scraping, credentialed collection, and exposure-search tooling**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Pattern 3: Tool-Allowlist Research Assistant (source identity preserved in pattern registry) - excludes broad scraping, credentialed collection, and exposure-search tooling**, reason from the sources cited in this row. [144, 2026] An AWS Prescriptive Guidance document (July 2025) introducing agentic AI patterns and workflows. It presents reusable design templates for building AI agent systems that operate with autonomy while remaining controllable and aligned with goals, aimed at architects, developers, and product leaders. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Pattern 3**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Pattern 3**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Pattern 3: Tool-Allowlist Research Assistant (source identity preserved in pattern registry) - excludes broad scraping, credentialed collection, and exposure-search tooling** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Pattern 3: Tool-Allowlist Research Assistant (source identity preserved in pattern registry) - excludes broad scraping, credentialed collection, and exposure-search tooling**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Pattern 3: Tool-Allowlist Research Assistant (source identity preserved in pattern registry) - excludes broad scraping, credentialed collection, and exposure-search tooling** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.10 Lesson 10: Safe methods: schema-bound tool calls, public-source retrieval, allowlisted connectors, and grounded summaries

Concept. Safe methods: schema-bound tool calls, public-source retrieval, allowlisted connectors, and grounded summaries evaluates retrieval pipelines by source provenance, injection risk, citation fidelity, and reviewer verification of answers.

Why it matters. Safe methods matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; treating pattern names as deployment playbooks is a common failure.

Source support. Safe methods: schema-bound tool calls, public-source retrieval, allowlisted connectors, and grounded summaries rests on [309, 2026], [310, 2026], and [300, 2026]. The most specific cited work observes: It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). Use them for fixing what **Safe methods: schema-bound tool calls, public-source retrieval, allowlisted connectors, and grounded summaries** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **Safe methods** against the works cited for this row. [309, 2026] An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection. [310, 2026] The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Safe methods**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe methods**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe methods** work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Safe methods**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe methods** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.11 Lesson 11: Safe defensive application: accountable bibliography, source inventory, or standards-mapping exercise

Concept. Safe defensive application: accountable bibliography, source inventory, or standards-mapping exercise uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. Safe defensive application connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Safe defensive application: accountable bibliography, source inventory, or standards-mapping exercise rests on [309, 2026], [310, 2026], and [300, 2026]. Its anchor reference records: The OASIS Standard specification for TAXII (Trusted Automated Exchange of

Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. Use them for pinning down the scope of **Safe defensive application: accountable bibliography, source inventory, or standards-mapping exercise**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Safe defensive application** in the evidence the row cites. [309, 2026] An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection. [310, 2026] The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Safe defensive application**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe defensive application**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe defensive application** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Safe defensive application**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe defensive application** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.12 Lesson 12: Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Tool-Allowlist Research Assistant Concept. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Tool-Allowlist Research Assistant

uses sharing standards to document indicator context, handling, confidence, and consumer responsibilities—not raw indicator hoarding.

Why it matters. Safe architecture artifact connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Tool-Allowlist Research Assistant rests on [309, 2026], [310, 2026], and [300, 2026]. The closest source to this row notes: It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). Use them for the claim that **Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Tool-Allowlist Research Assistant** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Safe architecture artifact**, work from the cited evidence behind this row. [309, 2026] An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection. [310, 2026] The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Safe architecture artifact**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe architecture artifact**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe architecture artifact** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Safe architecture artifact**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe architecture artifact** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.13 Lesson 13: Pattern 4: Governed Planner-Executor (source identity preserved in pattern registry) - plans curriculum artifacts only and does not create live operational tasking Concept. Pattern 4: Governed Planner-Executor (source identity preserved in pattern registry) - plans curriculum artifacts only and does not create live operational tasking

uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Analysts use **Pattern 4: Governed Planner-Executor (source identity preserved in pattern registry) - plans curriculum artifacts only and does not create live operational tasking** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that treating pattern names as deployment playbooks would otherwise hide, and the reviewer accountable for challenge.

Source support. Pattern 4: Governed Planner-Executor (source identity preserved in pattern registry) - plans curriculum artifacts only and does not create live operational tasking rests on [139, 2026] and [145, 2026]. The lead source's own note reads: This is an arXiv research paper by Sivasathivel Kandasamy titled "Control Plane as a Tool: A Scalable Design Pattern for Agentic AI Systems." It proposes an architectural pattern in which AI agents interact with a single control-plane interface that handles tool routing and selection, rather than exposing many tools directly. Use them for the claim that **Pattern 4: Governed Planner-Executor (source identity preserved in pattern registry) - plans curriculum artifacts only and does not create live operational tasking** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Pattern 4: Governed Planner-Executor (source identity preserved in pattern registry) - plans curriculum artifacts only and does not create live operational tasking**, work from the cited evidence behind this row. [139, 2026] A LinkedIn post by Aishwarya Srinivasan discussing agentic AI design patterns for building production-grade AI agents. [145, 2026] This is an arXiv research paper by Sivasathivel Kandasamy titled "Control Plane as a Tool: A Scalable Design Pattern for Agentic AI Systems." It proposes an architectural pattern in which AI agents interact with a single control-plane interface that handles tool routing and selection, rather than exposing many tools directly. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Pattern 4**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Pattern 4**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Pattern 4: Governed Planner-Executor (source identity preserved in pattern registry) - plans curriculum artifacts only and does not create live operational tasking** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and

the stop condition.

Misconception check. Correct the misconception about **Pattern 4: Governed Planner-Executor (source identity preserved in pattern registry) - plans curriculum artifacts only and does not create live operational tasking**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Pattern 4: Governed Planner-Executor (source identity preserved in pattern registry) - plans curriculum artifacts only and does not create live operational tasking** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.14 Lesson 14: Safe methods: milestone decomposition, approval gates, dependency checks, and rollback notes

Concept. Safe methods: milestone decomposition, approval gates, dependency checks, and rollback notes connects cognitive science claims to analytic bias literacy: what the brain prioritizes, what it misses, and how review compensates.

Why it matters. Safe methods connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Safe methods: milestone decomposition, approval gates, dependency checks, and rollback notes rests on [299, 2026], [306, 2026], and [312, 2026]. The most specific cited work observes: It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). Use them for the claim that **Safe methods: milestone decomposition, approval gates, dependency checks, and rollback notes** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Safe methods**, reason from the sources cited in this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Safe methods**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe methods**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe methods** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe methods** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.15 Lesson 15: Safe defensive application: classroom project plan for evidence review, policy analysis, or tabletop preparation

Concept. Safe defensive application: classroom project plan for evidence review, policy analysis, or tabletop preparation — Match intelligence requirements to least-intrusive source disciplines with explicit minimization and feedback to the customer.

Why it matters. Safe defensive application connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Safe defensive application: classroom project plan for evidence review, policy analysis, or tabletop preparation rests on [309, 2026], [310, 2026], and [300, 2026]. The most specific cited work observes: It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). Use them for fixing what **Safe defensive application: classroom project plan for evidence review, policy analysis, or tabletop preparation** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Safe defensive application**, work from the cited evidence behind this row. [309, 2026] An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection. [310, 2026] The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Safe defensive application**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe defensive application**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe defensive application** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Safe defensive application**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe defensive application** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.16 Lesson 16: Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Governed Planner-Executor

Concept. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Governed Planner-Executor uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Safe architecture artifact connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Governed Planner-Executor rests on [299, 2026], [306, 2026], and [312, 2026]. The closest source to this row notes: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for fixing what **Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Governed Planner-Executor** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Safe architecture artifact**, work from the cited evidence behind this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-

infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Safe architecture artifact**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe architecture artifact**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe architecture artifact** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Safe architecture artifact**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe architecture artifact** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.17 Lesson 17: Pattern 5: Parallel Source-Corroboration Agent (source identity preserved in pattern registry) - uses public or provided materials and avoids intelligence collection expansion

Concept. Pattern 5: Parallel Source-Corroboration Agent (source identity preserved in pattern registry) - uses public or provided materials and avoids intelligence collection expansion uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Pattern 5: Parallel Source-Corroboration Agent (source identity preserved in pattern registry) - uses public or provided materials and avoids intelligence collection expansion matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; treating pattern names as deployment playbooks is a common failure.

Source support. Pattern 5: Parallel Source-Corroboration Agent (source identity preserved in pattern registry) - uses public or provided materials and avoids intelligence collection expansion rests on [144, 2026]. The closest source to this row notes: An AWS Prescriptive Guidance document (July 2025) introducing agentic AI patterns and workflows. Use it for the working definition that **Pattern 5: Parallel Source-Corroboration Agent (source identity preserved in pattern registry) - uses public or provided materials and avoids intelligence collection expansion** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Pattern 5: Parallel Source-Corroboration Agent (source identity preserved in pattern registry) - uses public or provided materials and avoids intelligence collection expansion**, work from the cited evidence behind this row. [144, 2026] An AWS Prescriptive Guidance document (July 2025) introducing agentic AI patterns and workflows. It presents reusable design templates for building AI agent systems that operate with autonomy while remaining controllable and aligned with goals, aimed at architects, developers, and product leaders. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Pattern 5**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Pattern 5**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Pattern 5: Parallel Source-Corroboration Agent (source identity preserved in pattern registry) - uses public or provided materials and avoids intelligence collection expansion** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Pattern 5: Parallel Source-Corroboration Agent (source identity preserved in pattern registry) - uses public or provided materials and avoids intelligence collection expansion**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Pattern 5: Parallel Source-Corroboration Agent (source identity preserved in pattern registry) - uses public or provided materials and avoids intelligence collection expansion** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.18 Lesson 18: Safe methods: bounded concurrent retrieval, deduplication, contradiction capture, and source descriptors

Concept. Safe methods: bounded concurrent retrieval, deduplication, contradiction capture, and source descriptors evaluates retrieval pipelines by source provenance, injection risk, citation fidelity, and reviewer verification of answers.

Why it matters. Safe methods connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Safe methods: bounded concurrent retrieval, deduplication, contradiction capture, and source descriptors rests on [299, 2026], [306, 2026], and [312, 2026]. The closest source to this row notes: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for pinning down the scope of **Safe methods: bounded concurrent retrieval, deduplication, contradiction capture, and source descriptors**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Safe methods**, work from the cited evidence behind this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Safe methods**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe methods**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe methods** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Safe methods**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe methods** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.19 Lesson 19: Safe defensive application: side-by-side comparison of public official, standards, and scholarly sources

Concept. Safe defensive application: side-by-side comparison of public official, standards, and scholarly sources frames SIGINT as authority-bound collection with minimization, handling rules, and communications-security implications.

Why it matters. Safe defensive application matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; treating pattern names as deployment playbooks is a common failure.

Source support. Safe defensive application: side-by-side comparison of public official, standards, and scholarly sources rests on [301, 2026] and [298, 2026]. The closest source to this row notes: Official Intelligence Community strategy for open-source intelligence governance, integration, source discovery, data, tools, tradecraft, and workforce priorities. Use them for the working definition that **Safe defensive application: side-by-side comparison of public official, standards, and scholarly sources** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Safe defensive application**, work from the cited evidence behind this row. [301, 2026] Official Intelligence Community strategy for open-source intelligence governance, integration, source discovery, data, tools, tradecraft, and workforce priorities. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Safe defensive application**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe defensive application**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe defensive application** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Safe defensive application**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe defensive application** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.20 Lesson 20: Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Parallel Source-Corroboration Agent

Concept. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Parallel Source-Corroboration Agent uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Without explicit treatment of **Safe architecture artifact**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Parallel Source-Corroboration Agent rests on [299, 2026], [306, 2026], and [312, 2026]. The most specific cited work observes: It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). Use them for fixing what **Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Parallel Source-Corroboration Agent** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Safe architecture artifact**, reason from the sources cited in this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Safe architecture artifact**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe architecture artifact**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe architecture artifact** work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Safe architecture artifact**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe architecture artifact** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.21 Lesson 21: Pattern 6: Role-Separated Review Crew (source identity preserved in pattern registry) - keeps roles educational, logged, and constrained to benign artifacts

Concept. Pattern 6: Role-Separated Review Crew (source identity preserved in pattern registry) - keeps roles educational, logged, and constrained to benign artifacts uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Analysts use **Pattern 6: Role-Separated Review Crew (source identity preserved in pattern registry) - keeps roles educational, logged, and constrained to benign artifacts** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that treating pattern names as deployment playbooks would otherwise hide, and the reviewer accountable for challenge.

Source support. Pattern 6: Role-Separated Review Crew (source identity preserved in pattern registry) - keeps roles educational, logged, and constrained to benign artifacts rests on [139, 2026] and [146, 2026]. The most specific cited work observes: It outlines core elements such as agent coordination, tool integration, memory management, workflow definition, and deployment monitoring, and reviews eight frameworks including LangGraph, AutoGen, CrewAI, LlamaIndex, Haystack, DSPy, and Semantic Kernel. Use them for the working definition that **Pattern 6: Role-Separated Review Crew (source identity preserved in pattern registry) - keeps roles educational, logged, and constrained to benign artifacts** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Pattern 6: Role-Separated Review Crew (source identity preserved in pattern registry) - keeps roles educational, logged, and constrained to benign artifacts** in the evidence the row cites. [139, 2026] A LinkedIn post by Aishwarya Srinivasan discussing agentic AI design patterns for building production-grade AI agents. [146, 2026] An Exabeam explainer describing agentic AI frameworks as software toolkits that provide pre-built components and architectures for building autonomous AI agents. It outlines core elements such as agent coordination, tool integration, memory management, workflow definition, and deployment monitoring, and reviews eight frameworks including LangGraph, AutoGen, CrewAI, LlamaIndex, Haystack, DSPy, and Semantic Kernel. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Pattern 6**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Pattern 6**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Pattern 6: Role-Separated Review Crew (source identity preserved in pattern registry) - keeps roles educational, logged, and constrained to benign artifacts** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Pattern 6: Role-Separated Review Crew (source identity preserved in pattern registry) - keeps roles educational, logged, and constrained to benign artifacts**: that naming an agent pattern certifies it is safe to deploy

without governance gates.

Transfer task. Transfer **Pattern 6: Role-Separated Review Crew (source identity preserved in pattern registry) - keeps roles educational, logged, and constrained to benign artifacts** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.22 Lesson 22: Safe methods: planner, retriever, validator, safety reviewer, and reporter roles

Concept. Safe methods: planner, retriever, validator, safety reviewer, and reporter roles uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. Safe methods connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Safe methods: planner, retriever, validator, safety reviewer, and reporter roles rests on [299, 2026], [306, 2026], and [312, 2026]. Its anchor reference records: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for the claim that **Safe methods: planner, retriever, validator, safety reviewer, and reporter roles** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Safe methods**, reason from the sources cited in this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Safe methods**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe methods**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe methods** work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Safe methods**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe methods** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.23 Lesson 23: Safe defensive application: tabletop red-team critique of an analytic memo, not an operational exercise

Concept. Safe defensive application: tabletop red-team critique of an analytic memo, not an operational exercise uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. Safe defensive application connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Safe defensive application: tabletop red-team critique of an analytic memo, not an operational exercise rests on [299, 2026], [306, 2026], and [312, 2026]. The lead source's own note reads: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for the claim that **Safe defensive application: tabletop red-team critique of an analytic memo, not an operational exercise** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Safe defensive application**, reason from the sources cited in this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Safe defensive application**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe defensive application**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe defensive application** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Safe defensive application**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe defensive application** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.24 Lesson 24: Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Role-Separated Review Crew

Concept. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Role-Separated Review Crew uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Without explicit treatment of **Safe architecture artifact**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Role-Separated Review Crew rests on [299, 2026], [306, 2026], and [312, 2026]. The closest source to this row notes: It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). Use them for the working definition that **Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Role-Separated Review Crew** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Safe architecture artifact**, work from the cited evidence behind this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Safe architecture artifact**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe architecture artifact**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable

for challenge. Shape **Safe architecture artifact** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Safe architecture artifact**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe architecture artifact** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.25 Lesson 25: Pattern 7: Competing-Hypotheses Debate Agent (source identity preserved in pattern registry) - does not generate adversarial persuasion or policy advocacy content

Concept. Pattern 7: Competing-Hypotheses Debate Agent (source identity preserved in pattern registry) - does not generate adversarial persuasion or policy advocacy content uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Pattern 7: Competing-Hypotheses Debate Agent (source identity preserved in pattern registry) - does not generate adversarial persuasion or policy advocacy content matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; treating pattern names as deployment playbooks is a common failure.

Source support. Pattern 7: Competing-Hypotheses Debate Agent (source identity preserved in pattern registry) - does not generate adversarial persuasion or policy advocacy content rests on [147, 2026]. The closest source to this row notes: Security analysis of major AI agent frameworks including LangChain, CrewAI, AutoGen, Semantic. Use it for the working definition that **Pattern 7: Competing-Hypotheses Debate Agent (source identity preserved in pattern registry) - does not generate adversarial persuasion or policy advocacy content** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Pattern 7: Competing-Hypotheses Debate Agent (source identity preserved in pattern registry) - does not generate adversarial persuasion or policy advocacy content**, work from the cited evidence behind this row. [147, 2026] Security analysis of major AI agent frameworks including LangChain, CrewAI, AutoGen, Semantic. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Pattern 7**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Pattern 7**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Pattern 7: Competing-Hypotheses Debate Agent (source identity preserved in pattern registry) - does not generate adversarial persuasion or policy advocacy content** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Pattern 7: Competing-Hypotheses Debate Agent (source identity preserved in pattern registry) - does not generate adversarial persuasion or policy advocacy content**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Pattern 7: Competing-Hypotheses Debate Agent (source identity preserved in pattern registry) - does not generate adversarial persuasion or policy advocacy content** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.26 Lesson 26: Safe methods: alternative generation, evidence challenge, dissent capture, and judge rubric

Concept. Safe methods: alternative generation, evidence challenge, dissent capture, and judge rubric uses structured devil's advocacy to surface disconfirming evidence and overconfidence before dissemination.

Why it matters. Safe methods connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Safe methods: alternative generation, evidence challenge, dissent capture, and judge rubric rests on [297, 2026] and [298, 2026]. The most specific cited work observes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for the claim that **Safe methods: alternative generation, evidence challenge, dissent capture, and judge rubric** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Safe methods**, work from the cited evidence behind this row. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Safe methods**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe methods**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe methods** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Safe methods**: that listing one favored hypothesis is enough without testing alternatives.

Transfer task. Transfer **Safe methods** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.27 Lesson 27: Safe defensive application: ACH-style review of a classroom claim with clearly separated evidence and judgment

Concept. Safe defensive application: ACH-style review of a classroom claim with clearly separated evidence and judgment uses the method to keep alternatives, disconfirming evidence, and confidence visible.

Why it matters. Safe defensive application matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; treating pattern names as deployment playbooks is a common failure.

Source support. Safe defensive application: ACH-style review of a classroom claim with clearly separated evidence and judgment rests on [297, 2026] and [298, 2026]. The most specific cited work observes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for the claim that **Safe defensive application: ACH-style review of a classroom claim with clearly separated evidence and judgment** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Safe defensive application** in the evidence the row cites. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Safe defensive application**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe defensive application**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for

challenge. Shape **Safe defensive application** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Safe defensive application**: that listing one favored hypothesis is enough without testing alternatives.

Transfer task. Transfer **Safe defensive application** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.28 Lesson 28: Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Competing-Hypotheses Debate Agent

Concept. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Competing-Hypotheses Debate Agent uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Safe architecture artifact connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Competing-Hypotheses Debate Agent rests on [299, 2026], [306, 2026], and [312, 2026]. Its anchor reference records: It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). Use them for fixing what **Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Competing-Hypotheses Debate Agent** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Safe architecture artifact** in the evidence the row cites. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Safe architecture artifact**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe architecture artifact**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe architecture artifact** work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Safe architecture artifact**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe architecture artifact** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.29 Lesson 29: Pattern 8: Provenance-Bound Retrieval Operator (source identity preserved in pattern registry) - does not connect to live sensitive stores or unapproved data collections

Concept. Pattern 8: Provenance-Bound Retrieval Operator (source identity preserved in pattern registry) - does not connect to live sensitive stores or unapproved data collections uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Without explicit treatment of **Pattern 8: Provenance-Bound Retrieval Operator (source identity preserved in pattern registry) - does not connect to live sensitive stores or unapproved data collections**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Pattern 8: Provenance-Bound Retrieval Operator (source identity preserved in pattern registry) - does not connect to live sensitive stores or unapproved data collections rests on [148, 2026]. The closest source to this row notes: This article by Riverside Research traces AI's evolution from large language models through retrieval-augmented systems, single-task agents, collaborative agentic systems, and toward emergent multi-agent autonomy capable of managing surveillance and decision support at operational speed. Use it for the working definition that **Pattern 8: Provenance-Bound Retrieval Operator (source identity preserved in pattern registry) - does not connect to live sensitive stores or unapproved data collections** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Pattern 8: Provenance-Bound Retrieval Operator (source identity preserved in pattern registry) - does not connect to live sensitive stores or unapproved data collections** in the evidence the row cites. [148, 2026] This article by Riverside Research traces AI's evolution from large language models through retrieval-augmented systems, single-task agents, collaborative agentic systems, and toward emergent multi-agent autonomy capable of managing surveillance and decision support at operational speed. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Pattern 8**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Pattern 8**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Pattern 8: Provenance-Bound Retrieval Operator (source identity preserved in pattern registry) - does not connect to live sensitive stores or unapproved data collections** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Pattern 8: Provenance-Bound Retrieval Operator (source identity preserved in pattern registry) - does not connect to live sensitive stores or unapproved data collections**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Pattern 8: Provenance-Bound Retrieval Operator (source identity preserved in pattern registry) - does not connect to live sensitive stores or unapproved data collections** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.30 Lesson 30: Safe methods: curated corpus retrieval, hybrid ranking, source snippets, and citation audits

Concept. Safe methods: curated corpus retrieval, hybrid ranking, source snippets, and citation audits evaluates retrieval pipelines by source provenance, injection risk, citation fidelity, and reviewer verification of answers.

Why it matters. Without explicit treatment of **Safe methods**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Safe methods: curated corpus retrieval, hybrid ranking, source snippets, and citation audits rests on [299, 2026], [306, 2026], and [312, 2026]. The lead source's own note reads: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for pinning down the scope of **Safe methods: curated corpus retrieval, hybrid ranking, source snippets, and citation audits**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Safe methods**, work from the cited evidence behind this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0

messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Safe methods**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe methods**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe methods** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Safe methods**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe methods** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.31 Lesson 31: Safe defensive application: course-pack retrieval over provided readings, standards, and official guidance Concept. Safe defensive application: course-pack retrieval over provided readings, standards, and official guidance evaluates retrieval pipelines by source provenance, injection risk, citation fidelity, and reviewer verification of answers.

Why it matters. Safe defensive application connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Safe defensive application: course-pack retrieval over provided readings, standards, and official guidance rests on [309, 2026], [310, 2026], and [300, 2026]. Its anchor reference records: The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. Use them for the working definition that **Safe defensive application: course-pack retrieval over provided readings, standards, and official guidance** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Safe defensive application** in the evidence the row cites. [309, 2026] An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection. [310, 2026] The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Safe defensive application**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe defensive application**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe defensive application** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Safe defensive application**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe defensive application** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.32 Lesson 32: Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Provenance-Bound Retrieval Operator Concept. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Provenance-Bound Retrieval Operator uses sharing standards to document indicator context, handling, confidence, and consumer responsibilities—not raw indicator hoarding.

Why it matters. Analysts use **Safe architecture artifact** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that treating pattern names as deployment playbooks would otherwise hide, and the reviewer accountable for challenge.

Source support. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Provenance-Bound Retrieval Operator rests on [309, 2026], [310, 2026], and [300, 2026]. Its anchor reference records: It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). Use them for the working definition that **Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Provenance-Bound Retrieval Operator** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **Safe architecture artifact** against the works cited for this row. [309, 2026] An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection. [310, 2026] The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Safe architecture artifact**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe architecture artifact**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe architecture artifact** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Safe architecture artifact**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe architecture artifact** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.33 Lesson 33: Pattern 9: Evidence-Memory State Machine (source identity preserved in pattern registry) - tracks claims and sources, not people, assets, or behavioral patterns Concept. Pattern 9: Evidence-Memory State Machine (source identity preserved in pattern registry) - tracks claims and sources, not people, assets, or behavioral patterns uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Pattern 9: Evidence-Memory State Machine (source identity preserved in pattern registry) - tracks claims and sources, not people, assets, or behavioral patterns connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Pattern 9: Evidence-Memory State Machine (source identity preserved in pattern registry) - tracks claims and sources, not people, assets, or behavioral patterns rests on [138, 2026]. The lead source's own note reads: An arXiv survey paper on agentic AI examining the shift from generative systems to autonomous agents that perceive, reason, plan, and act. Use it for the working definition that **Pattern 9: Evidence-Memory State Machine (source identity preserved in pattern registry) - tracks claims and sources, not people, assets, or behavioral patterns** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Pattern 9: Evidence-Memory State Machine (source identity preserved in pattern registry) - tracks claims and sources, not people, assets, or behavioral patterns**, reason from the sources cited in this row. [138, 2026] An arXiv survey paper on agentic AI examining the shift from generative systems to autonomous agents that perceive, reason, plan, and act. It proposes a unified taxonomy decomposing LLM-based agents into six dimensions: core components, cognitive architecture, learning paradigms, multi-agent systems, environments

and domains, and evaluation and safety. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Pattern 9**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Pattern 9**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Pattern 9: Evidence-Memory State Machine (source identity preserved in pattern registry) - tracks claims and sources, not people, assets, or behavioral patterns** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Pattern 9: Evidence-Memory State Machine (source identity preserved in pattern registry) - tracks claims and sources, not people, assets, or behavioral patterns**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Pattern 9: Evidence-Memory State Machine (source identity preserved in pattern registry) - tracks claims and sources, not people, assets, or behavioral patterns** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.34 Lesson 34: Safe methods: episodic note cards, retention limits, consolidation, and source change logs

Concept. Safe methods: episodic note cards, retention limits, consolidation, and source change logs connects cognitive science claims to analytic bias literacy: what the brain prioritizes, what it misses, and how review compensates.

Why it matters. Without explicit treatment of **Safe methods**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Safe methods: episodic note cards, retention limits, consolidation, and source change logs rests on [299, 2026], [306, 2026], and [312, 2026]. The closest source to this row notes: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for pinning down the scope of **Safe methods: episodic note cards, retention limits, consolidation, and source change logs**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Safe methods** in the evidence the row cites. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Safe methods**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe methods**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe methods** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Safe methods**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe methods** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.35 Lesson 35: Safe defensive application: longitudinal claim ledger for curriculum evidence and revision history

Concept. Safe defensive application: longitudinal claim ledger for curriculum evidence and revision history uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. Without explicit treatment of **Safe defensive application**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Safe defensive application: longitudinal claim ledger for curriculum evidence and revision history rests on [299, 2026], [306, 2026], and [312, 2026]. The closest source to this row notes: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for the claim that **Safe defensive application: longitudinal claim ledger for curriculum evidence and revision history** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **Safe defensive application** against the works cited for this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Safe defensive application**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe defensive application**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe defensive application** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Safe defensive application**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe defensive application** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.36 Lesson 36: Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Evidence-Memory State Machine

Concept. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Evidence-Memory State Machine uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Without explicit treatment of **Safe architecture artifact**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Evidence-Memory State Machine rests on [299, 2026], [306, 2026], and [312, 2026]. Its anchor reference records: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for fixing what **Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Evidence-Memory State Machine** covers,

marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Safe architecture artifact**, work from the cited evidence behind this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Safe architecture artifact**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe architecture artifact**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe architecture artifact** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Safe architecture artifact**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe architecture artifact** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.37 Lesson 37: Pattern 10: Permissioned Control Plane Agent (source identity preserved in pattern registry) - keeps every tool revocable, observable, and constrained to evidence-bounded actions

Concept. Pattern 10: Permissioned Control Plane Agent (source identity preserved in pattern registry) - keeps every tool revocable, observable, and constrained to evidence-bounded actions uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Pattern 10: Permissioned Control Plane Agent (source identity preserved in pattern registry) - keeps every tool revocable, observable, and constrained to evidence-bounded actions matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; treating pattern names as deployment playbooks is a common failure.

Source support. Pattern 10: Permissioned Control Plane Agent (source identity preserved in pattern registry) - keeps every tool revocable, observable, and constrained to evidence-bounded actions rests on [145, 2026]. The most specific cited work observes: This is an arXiv research paper by Sivasathivel Kandasamy titled "Control Plane as a Tool: A Scalable Design Pattern for Agentic AI Systems." It proposes an architectural pattern in which AI agents interact with a single control-plane interface that handles tool routing and selection, rather than exposing many tools directly. Use it for the claim that **Pattern 10: Permissioned Control Plane Agent (source identity preserved in pattern registry) - keeps every tool revocable, observable, and constrained to evidence-bounded actions** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Pattern 10: Permissioned Control Plane Agent (source identity preserved in pattern registry) - keeps every tool revocable, observable, and constrained to evidence-bounded actions**, reason from the sources cited in this row. [145, 2026] This is an arXiv research paper by Sivasathivel Kandasamy titled "Control Plane as a Tool: A Scalable Design Pattern for Agentic AI Systems." It proposes an architectural pattern in which AI agents interact with a single control-plane interface that handles tool routing and selection, rather than exposing many tools directly. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Pattern 10**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Pattern 10**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Pattern 10: Permissioned Control Plane Agent (source identity preserved in pattern registry) - keeps every tool revocable, observable, and constrained to evidence-bounded actions** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Pattern 10: Permissioned Control Plane Agent (source identity preserved in pattern registry) - keeps every tool revocable, observable, and constrained to evidence-bounded actions**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Pattern 10: Permissioned Control Plane Agent (source identity preserved in pattern registry) - keeps every tool revocable, observable, and constrained to evidence-bounded actions** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.38 Lesson 38: Safe methods: single-interface routing, policy checks, budget limits, and audit logs

Concept. Safe methods: single-interface routing, policy checks, budget limits, and audit logs uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. Without explicit treatment of **Safe methods**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Safe methods: single-interface routing, policy checks, budget limits, and audit logs rests on [309, 2026], [310, 2026], and [300, 2026]. The lead source's own note reads: The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. Use them for fixing what **Safe methods: single-interface routing, policy checks, budget limits, and audit logs** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Safe methods**, work from the cited evidence behind this row. [309, 2026] An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection. [310, 2026] The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Safe methods**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe methods**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe methods** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Safe methods**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe methods** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.39 Lesson 39: Safe defensive application: tool-governance demo that routes among benign summarization and validation utilities Concept. Safe defensive application: tool-governance demo that routes among benign summarization and validation utilities uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. Analysts use **Safe defensive application** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that treating pattern names as deployment playbooks would otherwise hide, and the reviewer accountable for challenge.

Source support. Safe defensive application: tool-governance demo that routes among benign summarization and validation utilities rests on [309, 2026], [310, 2026], and [300, 2026]. The closest source to this row notes: It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). Use them for the claim that **Safe defensive application: tool-governance demo that routes among benign summarization and validation utilities** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Safe defensive application** in the evidence the row cites. [309, 2026] An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection. [310, 2026] The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Safe defensive application**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe defensive application**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe defensive application** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe defensive application** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.40 Lesson 40: Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Permissioned Control Plane Agent Concept. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Permissioned Control Plane Agent uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Safe architecture artifact connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Permissioned Control Plane Agent rests on [299, 2026], [306, 2026], and [312, 2026]. The closest source to this row notes: It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). Use them for the claim that **Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Permissioned Control Plane Agent** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Safe architecture artifact** in the evidence the row cites. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Safe architecture artifact**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe architecture artifact**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe architecture artifact** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Safe architecture artifact**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe architecture artifact** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.41 Lesson 41: Pattern 11: Monitoring-Governance Tabletop Agent (source identity preserved in pattern registry) - prohibits tracking real people, real targets, private forums, or infrastructure Concept. Pattern 11: Monitoring-Governance Tabletop Agent (source identity preserved in pattern registry) - prohibits tracking real people, real targets, private forums, or infrastructure uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Pattern 11: Monitoring-Governance Tabletop Agent (source identity preserved in pattern registry) - prohibits tracking real people, real targets, private forums, or infrastructure matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; treating pattern names as deployment playbooks is a common failure.

Source support. Pattern 11: Monitoring-Governance Tabletop Agent (source identity preserved in pattern registry) - prohibits tracking real people, real targets, private forums, or infrastructure rests on [299, 2026], [306, 2026], and [312, 2026]. The lead source's own note reads: It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). Use them for the claim that **Pattern 11: Monitoring-Governance Tabletop Agent (source identity preserved in pattern registry) - prohibits tracking real people, real targets, private forums, or infrastructure** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Pattern 11: Monitoring-Governance Tabletop Agent (source identity preserved in pattern registry) - prohibits tracking real people, real targets, private forums, or infrastructure**, work from the cited evidence behind this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data

sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Pattern 11**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Pattern 11**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Pattern 11: Monitoring-Governance Tabletop Agent (source identity preserved in pattern registry) - prohibits tracking real people, real targets, private forums, or infrastructure** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Pattern 11: Monitoring-Governance Tabletop Agent (source identity preserved in pattern registry) - prohibits tracking real people, real targets, private forums, or infrastructure** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.42 Lesson 42: Safe methods: synthetic event polling, threshold rationale, alert review, and escalation logging

Concept. Safe methods: synthetic event polling, threshold rationale, alert review, and escalation logging uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. Without explicit treatment of **Safe methods**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Safe methods: synthetic event polling, threshold rationale, alert review, and escalation logging rests on [309, 2026], [310, 2026], and [300, 2026]. The lead source's own note reads: The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. Use them for the working definition that **Safe methods: synthetic event polling, threshold rationale, alert review, and escalation logging** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **Safe methods** against the works cited for this row. [309, 2026] An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection. [310, 2026] The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Safe methods**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe methods**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe methods** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Safe methods**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe methods** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.43 Lesson 43: Safe defensive application: accountable monitoring governance exercise over toy asset-health records

Concept. Safe defensive application: accountable monitoring governance exercise over toy asset-health records — Discuss dark-web sources only through governance: legality, safety, provenance limits, and instructor-provided synthetic records.

Why it matters. Without explicit treatment of **Safe defensive application**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Safe defensive application: accountable monitoring governance exercise over toy asset-health records rests on [299, 2026], [306, 2026], and [312, 2026]. The closest source to this row notes: It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). Use them for the working definition that **Safe defensive application: accountable monitoring governance exercise over toy asset-health records** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Safe defensive application** in the evidence the row cites. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Safe defensive application**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe defensive application**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe defensive application** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe defensive application** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.44 Lesson 44: Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Monitoring-Governance Tabletop Agent

Concept. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Monitoring-Governance Tabletop Agent uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Analysts use **Safe architecture artifact** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that treating pattern names as deployment playbooks would otherwise hide, and the reviewer accountable for challenge.

Source support. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Monitoring-Governance Tabletop Agent rests on [307, 2026], [305, 2026], and [304, 2026]. The lead source's own note reads: NIST SP 800-218, the Secure Software Development

Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Use them for fixing what **Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Monitoring-Governance Tabletop Agent** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Safe architecture artifact**, work from the cited evidence behind this row. [307, 2026] Official CISA Industrial Control Systems recommended practices page for defensive ICS/OT safety, resilience, and incident-preparation guidance. [305, 2026] Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Safe architecture artifact**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe architecture artifact**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe architecture artifact** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe architecture artifact** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.45 Lesson 45: Pattern 12: Control-Coverage Critique Agent (source identity preserved in pattern registry) - does not automate exploitation, weakness discovery, or attack-chain execution

Concept. Pattern 12: Control-Coverage Critique Agent (source identity preserved in pattern registry) - does not automate exploitation, weakness discovery, or attack-chain execution uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Pattern 12: Control-Coverage Critique Agent (source identity preserved in pattern registry) - does not automate exploitation, weakness discovery, or attack-chain execution connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Pattern 12: Control-Coverage Critique Agent (source identity preserved in pattern registry) - does not automate exploitation, weakness discovery, or attack-chain execution rests on [147, 2026]. The most specific cited work observes: Security analysis of major AI agent frameworks including LangChain, CrewAI, AutoGen, Semantic. Use it for pinning down the scope of **Pattern 12: Control-Coverage Critique Agent (source identity preserved in pattern registry) - does not automate exploitation, weakness discovery, or attack-chain execution**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Pattern 12: Control-Coverage Critique Agent (source identity preserved in pattern registry) - does not automate exploitation, weakness discovery, or attack-chain execution**, work from the cited evidence behind this row. [147, 2026] Security analysis of major AI agent frameworks including LangChain, CrewAI, AutoGen, Semantic. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Pattern 12**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Pattern 12**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Pattern 12: Control-Coverage Critique Agent (source identity preserved in pattern registry) - does not automate exploitation, weakness discovery, or attack-chain execution** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Pattern 12: Control-Coverage Critique Agent (source identity preserved in pattern registry) - does not automate exploitation, weakness discovery, or attack-chain execution**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Pattern 12: Control-Coverage Critique Agent (source identity preserved in pattern registry) - does not automate exploitation, weakness discovery, or attack-chain execution** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.46 Lesson 46: Safe methods: policy-safe scenario cards, control mapping, misuse-case review, and mitigation scoring

Concept. Safe methods: policy-safe scenario cards, control mapping, misuse-case review, and mitigation scoring uses the model as defensive vocabulary for sequencing observations, not as a checklist of adversary actions.

Why it matters. Safe methods connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Safe methods: policy-safe scenario cards, control mapping, misuse-case review, and mitigation scoring rests on [300, 2026], [304, 2026], and [306, 2026]. The most specific cited work observes: NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Use them for the claim that **Safe methods: policy-safe scenario cards, control mapping, misuse-case review, and mitigation scoring** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Safe methods**, work from the cited evidence behind this row. [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Safe methods**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe methods**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe methods** work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Safe methods**: that a defensive taxonomy is an instruction sequence.

Transfer task. Transfer **Safe methods** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.47 Lesson 47: Safe defensive application: defensive tabletop review of controls against published high-level tactics

Concept. Safe defensive application: defensive tabletop review of controls against published high-level tactics treats the vulnerability record as

an assurance case: severity, affected component, provenance, mitigation status, and uncertainty stay separate.

Why it matters. Without explicit treatment of **Safe defensive application**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Safe defensive application: defensive tabletop review of controls against published high-level tactics rests on [300, 2026], [304, 2026], and [306, 2026]. The closest source to this row notes: NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Use them for the working definition that **Safe defensive application: defensive tabletop review of controls against published high-level tactics** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Safe defensive application**, work from the cited evidence behind this row. [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Safe defensive application**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe defensive application**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe defensive application** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Safe defensive application**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe defensive application** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.48 Lesson 48: Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Control-Coverage Critique Agent

Concept. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Control-Coverage Critique Agent uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Safe architecture artifact connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Control-Coverage Critique Agent rests on [300, 2026], [304, 2026], and [306, 2026]. Its anchor reference records: NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Use them for fixing what **Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Control-Coverage Critique Agent** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **Safe architecture artifact** against the works cited for this row. [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Safe architecture artifact**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe architecture artifact**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe architecture artifact** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Safe architecture artifact**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe architecture artifact** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.49 Lesson 49: Pattern 13: Identity-and-Provenance Fiction Audit (source identity preserved in pattern registry) - prohibits impersonation, false identity creation, and operational-security support

Concept. Pattern 13: Identity-and-Provenance Fiction Audit (source identity preserved in pattern registry) - prohibits impersonation, false identity creation, and operational-security support uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Without explicit treatment of **Pattern 13: Identity-and-Provenance Fiction Audit (source identity preserved in pattern registry) - prohibits impersonation, false identity creation, and operational-security support**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Pattern 13: Identity-and-Provenance Fiction Audit (source identity preserved in pattern registry) - prohibits impersonation, false identity creation, and operational-security support rests on [299, 2026], [306, 2026], and [312, 2026]. The lead source's own note reads: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for the working definition that **Pattern 13: Identity-and-Provenance Fiction Audit (source identity preserved in pattern registry) - prohibits impersonation, false identity creation, and operational-security support** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **Pattern 13: Identity-and-Provenance Fiction Audit (source identity preserved in pattern registry) - prohibits impersonation, false identity creation, and operational-security support** against the works cited for this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Each source above earns its place in this topic only when you can state

its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Pattern 13**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Pattern 13**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Pattern 13: Identity-and-Provenance Fiction Audit (source identity preserved in pattern registry) - prohibits impersonation, false identity creation, and operational-security support** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Pattern 13: Identity-and-Provenance Fiction Audit (source identity preserved in pattern registry) - prohibits impersonation, false identity creation, and operational-security support**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Pattern 13: Identity-and-Provenance Fiction Audit (source identity preserved in pattern registry) - prohibits impersonation, false identity creation, and operational-security support** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.50 Lesson 50: Safe methods: synthetic persona-risk critique, provenance labeling, and consistency-error detection **Concept. Safe methods: synthetic persona-risk critique, provenance labeling, and consistency-error detection** uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. Analysts use **Safe methods** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that treating pattern names as deployment playbooks would otherwise hide, and the reviewer accountable for challenge.

Source support. Safe methods: synthetic persona-risk critique, provenance labeling, and consistency-error detection rests on [299, 2026], [306, 2026], and [312, 2026]. The lead source's own note reads: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for pinning down the scope of **Safe methods: synthetic persona-risk critique, provenance labeling, and consistency-error detection**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Safe methods** in the evidence the row cites. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Safe methods**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe methods**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe methods** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Safe methods**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe methods** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.51 Lesson 51: Safe defensive application: ethics exercise that detects fabricated identity artifacts in clearly synthetic materials **Concept. Safe defensive application: ethics exercise that detects fabricated identity artifacts in clearly synthetic materials** uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. Safe defensive application matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; treating pattern names as deployment playbooks is a common failure.

Source support. Safe defensive application: ethics exercise that detects fabricated identity artifacts in clearly synthetic materials rests on [299, 2026], [306, 2026], and [312, 2026]. The lead source's own note reads: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for fixing what **Safe defensive application: ethics exercise that detects fabricated identity artifacts in clearly synthetic materials** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Safe defensive application** in the evidence the row cites. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Safe defensive application**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe defensive application**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe defensive application** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Safe defensive application**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe defensive application** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.52 Lesson 52: Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Identity-and-Provenance Fiction Audit **Concept. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Identity-and-Provenance Fiction Audit** uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Without explicit treatment of **Safe architecture artifact**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Identity-and-Provenance Fiction Audit rests on [299, 2026], [306, 2026], and [312, 2026]. The closest source to this row notes: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for pinning down the scope of **Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Identity-and-**

Provenance Fiction Audit, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **Safe architecture artifact** against the works cited for this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Safe architecture artifact**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe architecture artifact**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe architecture artifact** work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Safe architecture artifact**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe architecture artifact** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.53 Lesson 53: Pattern 14: Source-Reliability Verification Agent (source identity preserved in pattern registry) - supports verification and does not accuse, deanonymize, or profile real people

Concept. Pattern 14: Source-Reliability Verification Agent (source identity preserved in pattern registry) - supports verification and does not accuse, deanonymize, or profile real people applies verification steps: source identity, chain, recency, corroboration, and explicit uncertainty before a claim enters analysis.

Why it matters. Without explicit treatment of **Pattern 14: Source-Reliability Verification Agent (source identity preserved in pattern registry) - supports verification and does not accuse, deanonymize, or profile real people**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Pattern 14: Source-Reliability Verification Agent (source identity preserved in pattern registry) - supports verification and does not accuse, deanonymize, or profile real people rests on [299, 2026], [306, 2026], and [312, 2026]. The closest source to this row notes: It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). Use them for the working definition that **Pattern 14: Source-Reliability Verification Agent (source identity preserved in pattern registry) - supports verification and does not accuse, deanonymize, or profile real people** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **Pattern 14: Source-Reliability Verification Agent (source identity preserved in pattern registry) - supports verification and does not accuse, deanonymize, or profile real people** against the works cited for this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Pattern 14**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Pattern 14**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Pattern 14: Source-Reliability Verification Agent (source identity preserved in pattern registry) - supports verification and does not accuse, deanonymize, or profile real people** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Pattern 14: Source-Reliability Verification Agent (source identity preserved in pattern registry) - supports verification and does not accuse, deanonymize, or profile real people**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Pattern 14: Source-Reliability Verification Agent (source identity preserved in pattern registry) - supports verification and does not accuse, deanonymize, or profile real people** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.54 Lesson 54: Safe methods: corroboration, metadata review, provenance checks, and content-authenticity labels

Concept. Safe methods: corroboration, metadata review, provenance checks, and content-authenticity labels treats metadata as a distinct evidence class with its own minimization, correlation limits, and legal review requirements.

Why it matters. Analysts use **Safe methods** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that treating pattern names as deployment playbooks would otherwise hide, and the reviewer accountable for challenge.

Source support. Safe methods: corroboration, metadata review, provenance checks, and content-authenticity labels rests on [309, 2026], [310, 2026], and [300, 2026]. Its anchor reference records: It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). Use them for the working definition that **Safe methods: corroboration, metadata review, provenance checks, and content-authenticity labels** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **Safe methods** against the works cited for this row. [309, 2026] An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection. [310, 2026] The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Safe methods**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe methods**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape

Safe methods work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Safe methods**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe methods** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.55 Lesson 55: Safe defensive application: public-source validation packet with uncertainty and review escalations

Concept. Safe defensive application: public-source validation packet with uncertainty and review escalations connects source-protection duties to reporting quality, compartmentation, and counterintelligence review without recreating handling tradecraft.

Why it matters. Safe defensive application matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; treating pattern names as deployment playbooks is a common failure.

Source support. Safe defensive application: public-source validation packet with uncertainty and review escalations rests on [308, 2026] and [311, 2026]. The closest source to this row notes: It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering. Use them for the claim that **Safe defensive application: public-source validation packet with uncertainty and review escalations** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Safe defensive application**, reason from the sources cited in this row. [308, 2026] An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure. [311, 2026] An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Safe defensive application**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe defensive application**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe defensive application** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Safe defensive application**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe defensive application** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.56 Lesson 56: Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Source-Reliability Verification Agent

Concept. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Source-Reliability Verification Agent applies verification steps: source identity, chain, recency, corroboration, and explicit uncertainty before a claim enters analysis.

Why it matters. Safe architecture artifact connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Source-Reliability Verification Agent rests on [299, 2026], [306, 2026], and [312, 2026]. Its anchor reference records: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for pinning down the scope of **Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Source-Reliability Verification Agent**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Safe architecture artifact** in the evidence the row cites. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Safe architecture artifact**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe architecture artifact**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe architecture artifact** work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Safe architecture artifact**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe architecture artifact** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.57 Lesson 57: Pattern 15: Analyst-in-the-Loop Review Agent (source identity preserved in pattern registry) - requires accountable human review before any external communication or decision

Concept. Pattern 15: Analyst-in-the-Loop Review Agent (source identity preserved in pattern registry) - requires accountable human review before any external communication or decision uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Without explicit treatment of **Pattern 15: Analyst-in-the-Loop Review Agent (source identity preserved in pattern registry) - requires accountable human review before any external communication or decision**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Pattern 15: Analyst-in-the-Loop Review Agent (source identity preserved in pattern registry) - requires accountable human review before any external communication or decision rests on [004, 2026]. The closest source to this row notes: He maintains that uniquely human qualities such as intuition, experience, and independent judgment become more valuable as adversaries gain access to the same AI tools. Use it for the working definition that **Pattern 15: Analyst-in-the-Loop Review Agent (source identity preserved in pattern registry) - requires accountable human review before any external communication or decision** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Pattern 15: Analyst-in-the-Loop Review Agent (source identity preserved in pattern registry) - requires accountable human review before any external communication or decision**, reason from the sources cited in this row. [004, 2026] Tom Mulligan argues that artificial intelligence will enhance rather than replace human intelligence professionals, contending that the future of intelligence

lies in human-machine collaboration. He maintains that uniquely human qualities such as intuition, experience, and independent judgment become more valuable as adversaries gain access to the same AI tools. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Pattern 15**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Pattern 15**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Pattern 15: Analyst-in-the-Loop Review Agent (source identity preserved in pattern registry) - requires accountable human review before any external communication or decision** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Pattern 15: Analyst-in-the-Loop Review Agent (source identity preserved in pattern registry) - requires accountable human review before any external communication or decision**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Pattern 15: Analyst-in-the-Loop Review Agent (source identity preserved in pattern registry) - requires accountable human review before any external communication or decision** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.58 Lesson 58: Safe methods: interrupt gates, confidence thresholds, human approvals, and audit handoffs **Concept. Safe methods: interrupt gates, confidence thresholds, human approvals, and audit handoffs** uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. Without explicit treatment of **Safe methods**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Safe methods: interrupt gates, confidence thresholds, human approvals, and audit handoffs rests on [297, 2026] and [298, 2026]. The closest source to this row notes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for the claim that **Safe methods: interrupt gates, confidence thresholds, human approvals, and audit handoffs** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Safe methods** in the evidence the row cites. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Safe methods**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe methods**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe methods** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe methods** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.59 Lesson 59: Safe defensive application: supervised classroom analysis workflow for compliance-constrained exercises **Concept. Safe defensive application: supervised classroom analysis workflow for compliance-constrained exercises** documents workflow stages with inputs, transforms, reviewers, and blocked actions at each handoff.

Why it matters. Safe defensive application matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; treating pattern names as deployment playbooks is a common failure.

Source support. Safe defensive application: supervised classroom analysis workflow for compliance-constrained exercises rests on [299, 2026], [306, 2026], and [312, 2026]. The most specific cited work observes: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for pinning down the scope of **Safe defensive application: supervised classroom analysis workflow for compliance-constrained exercises**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Safe defensive application** in the evidence the row cites. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Safe defensive application**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe defensive application**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe defensive application** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Safe defensive application**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe defensive application** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.60 Lesson 60: Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Analyst-in-the-Loop Review Agent **Concept. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Analyst-in-the-Loop Review Agent** uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Safe architecture artifact matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; treating pattern names as deployment playbooks is a common failure.

Source support. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Analyst-in-the-Loop Review Agent rests on [299, 2026], [306, 2026], and [312, 2026]. The closest source to this row notes: It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). Use them for the working definition that **Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Analyst-in-the-Loop Review Agent** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Safe architecture artifact**, work from the cited evidence behind this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Safe architecture artifact**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe architecture artifact**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe architecture artifact** work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Safe architecture artifact**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe architecture artifact** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.61 Lesson 61: Pattern 16: SOC Tabletop Triage Agent (source identity preserved in pattern registry) - does not run response actions, touch production systems, or publish indicators as fact

Concept. Pattern 16: SOC Tabletop Triage Agent (source identity preserved in pattern registry) - does not run response actions, touch production systems, or publish indicators as fact uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Pattern 16: SOC Tabletop Triage Agent (source identity preserved in pattern registry) - does not run response actions, touch production systems, or publish indicators as fact matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; treating pattern names as deployment playbooks is a common failure.

Source support. Pattern 16: SOC Tabletop Triage Agent (source identity preserved in pattern registry) - does not run response actions, touch production systems, or publish indicators as fact rests on [149, 2026] and [150, 2026]. Its anchor reference records: An article from Cybersecurity Tribe examining where autonomous AI should and should not operate within security operations, drawing on survey data and commentary from numerous security experts. Use them for fixing what **Pattern 16: SOC Tabletop Triage Agent (source identity preserved in pattern registry) - does not run response actions, touch production systems, or publish indicators as fact** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Pattern 16: SOC Tabletop Triage Agent (source identity preserved in pattern registry) - does not run response actions, touch production systems, or publish indicators as fact** in the evidence the row cites. [149, 2026] A 2025 blog article from Simbian AI explaining the application of agentic AI to security operations centers. It describes an architecture organized into perception, cognitive, and action modules, and a coordinated framework of specialized agents for tasks such as alert triage, threat investigation, and vulnerability management. [150, 2026] An article from Cybersecurity Tribe examining where autonomous AI should and should not operate within security operations, drawing on survey data and commentary from numerous security experts. It identifies high-volume, repetitive tasks such as alert triage and policy validation as well suited to automation, while warning against autonomous handling of irreversible or high-impact decisions affecting infrastructure and access. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Pattern 16**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Pattern 16**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Pattern 16: SOC Tabletop Triage Agent (source identity preserved in pattern registry) - does not run response actions, touch production systems, or publish indicators as fact** work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Pattern 16: SOC Tabletop Triage Agent (source identity preserved in pattern registry) - does not run response actions, touch production systems, or publish indicators as fact**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Pattern 16: SOC Tabletop Triage Agent (source identity preserved in pattern registry) - does not run response actions, touch production systems, or publish indicators as fact** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.62 Lesson 62: Safe methods: synthetic alert enrichment, ATT&CK mapping, severity rationale, and debrief notes

Concept. Safe methods: synthetic alert enrichment, ATT&CK mapping, severity rationale, and debrief notes uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. Safe methods connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Safe methods: synthetic alert enrichment, ATT&CK mapping, severity rationale, and debrief notes rests on [302, 2026] and [297, 2026]. The most specific cited work observes: Department of Defense and intelligence community organization. Use them for pinning down the scope of **Safe methods: synthetic alert enrichment, ATT&CK mapping, severity rationale, and debrief notes**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Safe methods** in the evidence the row cites. [302, 2026] The official "About Us" page of the National Geospatial-Intelligence Agency (NGA), a U.S. Department of Defense and intelligence community organization. It describes NGA's mission of delivering geospatial intelligence, or GEOINT, to support military operations, policymakers, and first responders, spanning imagery analysis, mapping, geodesy, and navigation safety. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Safe methods**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe methods**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe methods** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Safe methods**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe methods** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.63 Lesson 63: Safe defensive application: tier-1 incident tabletop over fabricated logs and published technique descriptions

Concept. Safe defensive application: tier-1 incident tabletop over fabricated logs and published technique descriptions uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. Without explicit treatment of **Safe defensive application**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Safe defensive application: tier-1 incident tabletop over fabricated logs and published technique descriptions rests on [299, 2026], [306, 2026], and [312, 2026]. The most specific cited work observes: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for the working definition that **Safe defensive application: tier-1 incident tabletop over fabricated logs and published technique descriptions** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **Safe defensive application** against the works cited for this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Safe defensive application**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe defensive application**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe defensive application** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Safe defensive application**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe defensive application** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.64 Lesson 64: Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for SOC Tabletop Triage Agent

Concept. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for SOC Tabletop Triage Agent uses sharing standards to document indicator context, handling, confidence, and consumer responsibilities—not raw indicator hoarding.

Why it matters. Safe architecture artifact connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for SOC Tabletop Triage Agent rests on [309, 2026], [310, 2026], and [300, 2026]. The closest source to this row notes: The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. Use them for the working definition that **Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for SOC Tabletop Triage Agent** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Safe architecture artifact** in the evidence the row cites. [309, 2026] An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection. [310, 2026] The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Safe architecture artifact**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded

claim about **Safe architecture artifact**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe architecture artifact** work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Safe architecture artifact**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe architecture artifact** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.65 Lesson 65: Pattern 17: Software Provenance Review Agent (source identity preserved in pattern registry) - does not hunt real maintainers or produce exploitability claims without evidence

Concept. Pattern 17: Software Provenance Review Agent (source identity preserved in pattern registry) - does not hunt real maintainers or produce exploitability claims without evidence shows how package provenance, social trust, build integrity, and assurance controls turn a software incident into reviewable evidence.

Why it matters. Pattern 17: Software Provenance Review Agent (source identity preserved in pattern registry) - does not hunt real maintainers or produce exploitability claims without evidence connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Pattern 17: Software Provenance Review Agent (source identity preserved in pattern registry) - does not hunt real maintainers or produce exploitability claims without evidence rests on [303, 2026], [304, 2026], and [305, 2026]. Its anchor reference records: An official NIST page on software supply chain security issued under Executive Order 14028, focused on the Software Bill of Materials as a formal record of software components and their supply chain. Use them for fixing what **Pattern 17: Software Provenance Review Agent (source identity preserved in pattern registry) - does not hunt real maintainers or produce exploitability claims without evidence** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Pattern 17: Software Provenance Review Agent (source identity preserved in pattern registry) - does not hunt real maintainers or produce exploitability claims without evidence** in the evidence the row cites. [303, 2026] An official NIST page on software supply chain security issued under Executive Order 14028, focused on the Software Bill of Materials as a formal record of software components and their supply chain. It explains the benefits of SBOMs for vulnerability identification and supply-chain transparency, recommends machine-readable formats such as SPDX, CycloneDX, and SWID, and describes foundational, sustaining, and enhancing levels of implementation. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. [305, 2026] Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Pattern 17**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Pattern 17**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Pattern 17: Software Provenance Review Agent (source identity preserved in pattern registry) - does not hunt real maintainers or produce exploitability claims without evidence** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Pattern 17: Software Provenance Review Agent (source identity preserved in pattern registry) - does not hunt real maintainers or produce exploitability claims without evidence** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.66 Lesson 66: Safe methods: SBOM reading, dependency graph review, advisory matching, and integrity questions

Concept. Safe methods: SBOM reading, dependency graph review, advisory matching, and integrity questions shows how package provenance, social trust, build integrity, and assurance controls turn a software incident into reviewable evidence.

Why it matters. Safe methods connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Safe methods: SBOM reading, dependency graph review, advisory matching, and integrity questions rests on [303, 2026], [304, 2026], and [305, 2026]. The lead source's own note reads: An official NIST page on software supply chain security issued under Executive Order 14028, focused on the Software Bill of Materials as a formal record of software components and their supply chain. Use them for the working definition that **Safe methods: SBOM reading, dependency graph review, advisory matching, and integrity questions** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Safe methods**, work from the cited evidence behind this row. [303, 2026] An official NIST page on software supply chain security issued under Executive Order 14028, focused on the Software Bill of Materials as a formal record of software components and their supply chain. It explains the benefits of SBOMs for vulnerability identification and supply-chain transparency, recommends machine-readable formats such as SPDX, CycloneDX, and SWID, and describes foundational, sustaining, and enhancing levels of implementation. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. [305, 2026] Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Safe methods**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe methods**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe methods** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Safe methods**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe methods** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.67 Lesson 67: Safe defensive application: defensive package-governance exercise over sample manifests and public advisories

Concept. Safe defensive application: defensive package-governance exercise over sample manifests and public advisories shows how package provenance, social trust, build integrity, and assurance controls turn a software incident into reviewable evidence.

Why it matters. Safe defensive application connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Safe defensive application: defensive package-governance exercise over sample manifests and public advisories rests on [076, 2026]. Its anchor reference records: In early 2024, a malicious backdoor was discovered embedded in XZ Utils, a widely used compression library

in Linux distributions, designed to enable unauthorized remote code execution via OpenSSH using an Ed448 private key. Use it for the working definition that **Safe defensive application: defensive package-governance exercise over sample manifests and public advisories** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Safe defensive application**, reason from the sources cited in this row. [076, 2026] In early 2024, a malicious backdoor was discovered embedded in XZ Utils, a widely used compression library in Linux distributions, designed to enable unauthorized remote code execution via OpenSSH using an Ed448 private key. The perpetrator, operating under the pseudonym Jia Tan, spent over two years building trust as a contributor before inserting the exploit, which received a maximum CVSS score of 10.0. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Safe defensive application**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe defensive application**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe defensive application** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe defensive application** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.68 Lesson 68: Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Software Provenance Review Agent

Concept. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Software Provenance Review Agent shows how package provenance, social trust, build integrity, and assurance controls turn a software incident into reviewable evidence.

Why it matters. Analysts use **Safe architecture artifact** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that treating pattern names as deployment playbooks would otherwise hide, and the reviewer accountable for challenge.

Source support. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Software Provenance Review Agent rests on [303, 2026], [304, 2026], and [305, 2026]. The lead source's own note reads: An official NIST page on software supply chain security issued under Executive Order 14028, focused on the Software Bill of Materials as a formal record of software components and their supply chain. Use them for the working definition that **Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Software Provenance Review Agent** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Safe architecture artifact**, work from the cited evidence behind this row. [303, 2026] An official NIST page on software supply chain security issued under Executive Order 14028, focused on the Software Bill of Materials as a formal record of software components and their supply chain. It explains the benefits of SBOMs for vulnerability identification and supply-chain transparency, recommends machine-readable formats such as SPDX, CycloneDX, and SWID, and describes foundational, sustaining, and enhancing levels of implementation. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. [305, 2026] Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Safe architecture artifact**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe architecture artifact**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe architecture artifact** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Safe architecture artifact**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe architecture artifact** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.69 Lesson 69: Pattern 18: GEOINT Data-Quality Audit Agent (source identity preserved in pattern registry) - limits work to non-sensitive metadata quality, uncertainty notes, and synthetic location examples

Concept. Pattern 18: GEOINT Data-Quality Audit Agent (source identity preserved in pattern registry) - limits work to non-sensitive metadata quality, uncertainty notes, and synthetic location examples treats metadata as a distinct evidence class with its own minimization, correlation limits, and legal review requirements.

Why it matters. Without explicit treatment of **Pattern 18: GEOINT Data-Quality Audit Agent (source identity preserved in pattern registry) - limits work to non-sensitive metadata quality, uncertainty notes, and synthetic location examples**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Pattern 18: GEOINT Data-Quality Audit Agent (source identity preserved in pattern registry) - limits work to non-sensitive metadata quality, uncertainty notes, and synthetic location examples rests on [302, 2026] and [297, 2026]. The closest source to this row notes: It describes NGA's mission of delivering geospatial intelligence, or GEOINT, to support military operations, policymakers, and first responders, spanning imagery analysis, mapping, geodesy, and navigation safety. Use them for the working definition that **Pattern 18: GEOINT Data-Quality Audit Agent (source identity preserved in pattern registry) - limits work to non-sensitive metadata quality, uncertainty notes, and synthetic location examples** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Pattern 18: GEOINT Data-Quality Audit Agent (source identity preserved in pattern registry) - limits work to non-sensitive metadata quality, uncertainty notes, and synthetic location examples**, reason from the sources cited in this row. [302, 2026] The official "About Us" page of the National Geospatial-Intelligence Agency (NGA), a U.S. Department of Defense and intelligence community organization. It describes NGA's mission of delivering geospatial intelligence, or GEOINT, to support military operations, policymakers, and first responders, spanning imagery analysis, mapping, geodesy, and navigation safety. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Pattern 18**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Pattern 18**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Pattern 18: GEOINT Data-Quality Audit Agent (source identity preserved in pattern registry) - limits work to non-sensitive metadata quality, uncertainty notes, and synthetic location examples** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Pattern 18: GEOINT Data-Quality Audit Agent (source identity preserved in**

pattern registry) - limits work to non-sensitive metadata quality, uncertainty notes, and synthetic location examples: that a visible feature is enough for a confident geospatial claim.

Transfer task. Transfer **Pattern 18: GEOINT Data-Quality Audit Agent (source identity preserved in pattern registry) - limits work to non-sensitive metadata quality, uncertainty notes, and synthetic location examples** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.70 Lesson 70: Safe methods: provided-image annotation, quality flags, geospatial metadata review, and caveat writing

Concept. Safe methods: provided-image annotation, quality flags, geospatial metadata review, and caveat writing treats metadata as a distinct evidence class with its own minimization, correlation limits, and legal review requirements.

Why it matters. Safe methods matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; treating pattern names as deployment playbooks is a common failure.

Source support. Safe methods: provided-image annotation, quality flags, geospatial metadata review, and caveat writing rests on [302, 2026] and [297, 2026]. The most specific cited work observes: Department of Defense and intelligence community organization. Use them for the claim that **Safe methods: provided-image annotation, quality flags, geospatial metadata review, and caveat writing** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Safe methods** in the evidence the row cites. [302, 2026] The official "About Us" page of the National Geospatial-Intelligence Agency (NGA), a U.S. Department of Defense and intelligence community organization. It describes NGA's mission of delivering geospatial intelligence, or GEOINT, to support military operations, policymakers, and first responders, spanning imagery analysis, mapping, geodesy, and navigation safety. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Safe methods**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe methods**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe methods** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Safe methods**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe methods** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.71 Lesson 71: Safe defensive application: synthetic imagery-change exercise focused on uncertainty and data quality

Concept. Safe defensive application: synthetic imagery-change exercise focused on uncertainty and data quality treats location evidence as a quality and uncertainty problem, separating map interpretation from targeting or attribution.

Why it matters. Safe defensive application connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Safe defensive application: synthetic imagery-change exercise focused on uncertainty and data quality rests on [299, 2026], [306, 2026], and [312, 2026]. The most specific cited work observes: It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). Use them for fixing what **Safe defensive application: synthetic imagery-change exercise focused on uncertainty and data quality** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Safe defensive application** in the evidence the row cites. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Safe defensive application**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe defensive application**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe defensive application** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Safe defensive application**: that a visible feature is enough for a confident geospatial claim.

Transfer task. Transfer **Safe defensive application** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.72 Lesson 72: Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for GEOINT Data-Quality Audit Agent

Concept. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for GEOINT Data-Quality Audit Agent treats location evidence as a quality and uncertainty problem, separating map interpretation from targeting or attribution.

Why it matters. Analysts use **Safe architecture artifact** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that treating pattern names as deployment playbooks would otherwise hide, and the reviewer accountable for challenge.

Source support. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for GEOINT Data-Quality Audit Agent rests on [299, 2026], [306, 2026], and [312, 2026]. Its anchor reference records: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for fixing what **Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for GEOINT Data-Quality Audit Agent** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **Safe architecture artifact** against the works cited for this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Safe architecture artifact**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded

claim about **Safe architecture artifact**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe architecture artifact** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Safe architecture artifact**: that a visible feature is enough for a confident geospatial claim.

Transfer task. Transfer **Safe architecture artifact** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.73 Lesson 73: Pattern 19: Cognitive-Resilience Education Agent (source identity preserved in pattern registry) - does not design persuasion campaigns, microtargeting, or covert influence content

Concept. Pattern 19: Cognitive-Resilience Education Agent (source identity preserved in pattern registry) - does not design persuasion campaigns, microtargeting, or covert influence content uses inoculation methods as evidence-informed, bounded, and context-dependent resilience education with transparent labels, source checks, non-manipulative corrections, and explicit measurement limits.

Why it matters. Without explicit treatment of **Pattern 19: Cognitive-Resilience Education Agent (source identity preserved in pattern registry) - does not design persuasion campaigns, microtargeting, or covert influence content**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Pattern 19: Cognitive-Resilience Education Agent (source identity preserved in pattern registry) - does not design persuasion campaigns, microtargeting, or covert influence content rests on [151, 2026]. The most specific cited work observes: Grounded in inoculation theory, it describes how exposing people to weakened forms of manipulative content can help them develop resistance before they encounter it in the wild. Use it for the claim that **Pattern 19: Cognitive-Resilience Education Agent (source identity preserved in pattern registry) - does not design persuasion campaigns, microtargeting, or covert influence content** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Pattern 19: Cognitive-Resilience Education Agent (source identity preserved in pattern registry) - does not design persuasion campaigns, microtargeting, or covert influence content**, work from the cited evidence behind this row. [151, 2026] A practitioner guide from Inoculation Science explaining prebunking as a proactive strategy to build preemptive resilience to misinformation. Grounded in inoculation theory, it describes how exposing people to weakened forms of manipulative content can help them develop resistance before they encounter it in the wild. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Pattern 19**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Pattern 19**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Pattern 19: Cognitive-Resilience Education Agent (source identity preserved in pattern registry) - does not design persuasion campaigns, microtargeting, or covert influence content** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Pattern 19: Cognitive-Resilience Education Agent (source identity preserved in pattern registry) - does not design persuasion campaigns, microtargeting, or covert influence content**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Pattern 19: Cognitive-Resilience Education Agent (source identity preserved in pattern registry) - does not design persuasion campaigns, microtargeting, or covert influence content** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.74 Lesson 74: Safe methods: manipulation-technique labeling, transparent prebunking, and audience-harm

Concept. Safe methods: manipulation-technique labeling, transparent prebunking, and audience-harm uses inoculation methods as evidence-informed, bounded, and context-dependent resilience education with transparent labels, source checks, non-manipulative corrections, and explicit measurement limits.

Why it matters. Without explicit treatment of **Safe methods**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Safe methods: manipulation-technique labeling, transparent prebunking, and audience-harm rests on [308, 2026] and [311, 2026]. Its anchor reference records: An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. Use them for pinning down the scope of **Safe methods: manipulation-technique labeling, transparent prebunking, and audience-harm**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Safe methods** in the evidence the row cites. [308, 2026] An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure. [311, 2026] An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Safe methods**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe methods**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe methods** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Safe methods**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe methods** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.75 Lesson 75: Safe defensive application: opt-in media-literacy micro-lesson for a sample classroom scenario

Concept. Safe defensive application: opt-in media-literacy micro-lesson for a sample classroom scenario compares resolution, accuracy, and temporal fitness before drawing a geospatial conclusion from imagery or map products.

Why it matters. Safe defensive application connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Safe defensive application: opt-in media-literacy micro-lesson for a sample classroom scenario rests on [152, 2026]. The closest source to this row notes: A University of Cambridge news article describing a large study, conducted with Bristol University and Google's Jigsaw, testing whether short animated videos can help people resist online manipulation. Use it for the claim that **Safe defensive application:**

opt-in media-literacy micro-lesson for a sample classroom scenario lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Safe defensive application** in the evidence the row cites. [152, 2026] A University of Cambridge news article describing a large study, conducted with Bristol University and Google's Jigsaw, testing whether short animated videos can help people resist online manipulation. The 90-second clips expose common manipulation techniques such as scapegoating, false dichotomies, and emotionally manipulative language, an approach the researchers call prebunking. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Safe defensive application**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe defensive application**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe defensive application** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Safe defensive application**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe defensive application** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.76 Lesson 76: Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Cognitive-Resilience Education Agent

Concept. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Cognitive-Resilience Education Agent uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Without explicit treatment of **Safe architecture artifact**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Cognitive-Resilience Education Agent rests on [305, 2026], [304, 2026], and [303, 2026]. The lead source's own note reads: An official NIST page on software supply chain security issued under Executive Order 14028, focused on the Software Bill of Materials as a formal record of software components and their supply chain. Use them for the working definition that **Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Cognitive-Resilience Education Agent** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Safe architecture artifact**, reason from the sources cited in this row. [305, 2026] Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. [303, 2026] An official NIST page on software supply chain security issued under Executive Order 14028, focused on the Software Bill of Materials as a formal record of software components and their supply chain. It explains the benefits of SBOMs for vulnerability identification and supply-chain transparency, recommends machine-readable formats such as SPDX, CycloneDX, and SWID, and describes foundational, sustaining, and enhancing levels of implementation. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Safe architecture artifact**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe architecture artifact**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe architecture artifact** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Safe architecture artifact**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe architecture artifact** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.77 Lesson 77: Pattern 20: Hierarchical Curriculum Orchestrator (source identity preserved in pattern registry) - orchestrates learning artifacts only and preserves human authorization gates

Concept. Pattern 20: Hierarchical Curriculum Orchestrator (source identity preserved in pattern registry) - orchestrates learning artifacts only and preserves human authorization gates uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Without explicit treatment of **Pattern 20: Hierarchical Curriculum Orchestrator (source identity preserved in pattern registry) - orchestrates learning artifacts only and preserves human authorization gates**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Pattern 20: Hierarchical Curriculum Orchestrator (source identity preserved in pattern registry) - orchestrates learning artifacts only and preserves human authorization gates rests on [139, 2026] and [137, 2026]. The lead source's own note reads: An arXiv paper surveying the shift from passive language models to Agentic AI, where large language models act as cognitive controllers that combine memory, tool use, and environmental feedback to pursue extended goals. Use them for the working definition that **Pattern 20: Hierarchical Curriculum Orchestrator (source identity preserved in pattern registry) - orchestrates learning artifacts only and preserves human authorization gates** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **Pattern 20: Hierarchical Curriculum Orchestrator (source identity preserved in pattern registry) - orchestrates learning artifacts only and preserves human authorization gates** against the works cited for this row. [139, 2026] A LinkedIn post by Aishwarya Srinivasan discussing agentic AI design patterns for building production-grade AI agents. [137, 2026] An arXiv paper surveying the shift from passive language models to Agentic AI, where large language models act as cognitive controllers that combine memory, tool use, and environmental feedback to pursue extended goals. It proposes a unified taxonomy organizing agent systems into six components: perception, brain, planning, action, tool use, and collaboration. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Pattern 20**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Pattern 20**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Pattern 20: Hierarchical Curriculum Orchestrator (source identity preserved in pattern registry) - orchestrates learning artifacts only and preserves human authorization gates** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Pattern 20: Hierarchical Curriculum Orchestrator (source identity preserved in pattern registry) - orchestrates learning artifacts only and preserves human authorization gates** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.78 Lesson 78: Safe methods: role delegation, output aggregation, exception routing, and failure recovery drills **Concept. Safe methods: role delegation, output aggregation, exception routing, and failure recovery drills** uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. Safe methods matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; treating pattern names as deployment playbooks is a common failure.

Source support. Safe methods: role delegation, output aggregation, exception routing, and failure recovery drills rests on [299, 2026], [306, 2026], and [312, 2026]. The most specific cited work observes: It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). Use them for fixing what **Safe methods: role delegation, output aggregation, exception routing, and failure recovery drills** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **Safe methods** against the works cited for this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Safe methods**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe methods**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe methods** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Safe methods**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe methods** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.79 Lesson 79: Safe defensive application: multi-domain capstone coordination across benign module artifacts **Concept. Safe defensive application: multi-domain capstone coordination across benign module artifacts** uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. Without explicit treatment of **Safe defensive application**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Safe defensive application: multi-domain capstone coordination across benign module artifacts rests on [299, 2026], [306, 2026], and [312, 2026]. The closest source to this row notes: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for fixing what **Safe defensive application: multi-domain capstone coordination across benign module artifacts** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Safe defensive application**, reason from the sources cited in this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Safe defensive application**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe defensive application**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe defensive application** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Safe defensive application**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Safe defensive application** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.2.80 Lesson 80: Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Hierarchical Curriculum Orchestrator **Concept. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Hierarchical Curriculum Orchestrator** uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Analysts use **Safe architecture artifact** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that treating pattern names as deployment playbooks would otherwise hide, and the reviewer accountable for challenge.

Source support. Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Hierarchical Curriculum Orchestrator rests on [299, 2026], [306, 2026], and [312, 2026]. The closest source to this row notes: It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). Use them for the claim that **Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Hierarchical Curriculum Orchestrator** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Safe architecture artifact**, work from the cited evidence behind this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Safe architecture artifact**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Safe architecture artifact**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Safe architecture artifact** work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Safe architecture artifact**: that naming an agent pattern certifies it is safe to deploy

without governance gates.

Transfer task. Transfer **Safe architecture artifact** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

46.2.3 AGEINT Design Patterns and Archetypes worked safe example: synthetic inputs, evidence, and review

Worked example: a synthetic research assistant agent organizes public readings for an instructor. [233, 2026]; [258, 2026].

Triangulation anchors. In module 32's worked-example section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **governed agentic intelligence**. Learners use a **agent run and assurance card** and keep this boundary visible: No autonomous external action, credentialed operations, live-target workflows, or uncontrolled tool use.

Frame. The classroom question centers on **Pattern 1: Focused Analytic Reasoner (source identity preserved in pattern registry) - keeps reasoning reviewable without exposing hidden reasoning or delegating action**. Excluded actions stay explicit, and the **Agentic Tool-Governance Lens** planning question is: Which human authority, agent identity, tool permission, autonomy limit, incident threshold, and recoverability condition bounds the workflow?

Inputs. For the **Pattern 1: Focused Analytic Reasoner** scenario, use public URLs, a fixed retrieval tool, a summarization prompt, a time budget, and a stop condition. The Agentic Tool-Governance Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Pattern 1: Focused Analytic Reasoner**, students bind the agent identity, list allowed tools, set autonomy limits, capture sources, block unsafe requests, and log approvals. Pause whenever an inference about Pattern 1: Focused Analytic Reasoner appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Pattern 1: Focused Analytic Reasoner** classroom scenario; unit artifact = agent run and assurance card; evidence = allowed inputs; method = least-privilege agent design and run review; output = an agent run card with tool calls, source links, blocked actions, reviewer notes, incident threshold, and recovery decision; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Pattern 1: Focused Analytic Reasoner** as "Agentic Tool-Governance Lens confirms it" is not enough. The revision ties the claim to least-privilege agent design and run review, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Pattern 1: Focused Analytic Reasoner** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

46.2.4 AGEINT Design Patterns and Archetypes practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Agentic Tool-Governance Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**.

Triangulation anchors. In module 32's practice-sequence section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Pattern 1: Focused Analytic Reasoner, Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes, Safe defensive application: single public-source report critique with provenance and uncertainty fields; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Agentic AI Governance and Tool Security** lane.
2. Frame	Answer the lens question: Which human authority, agent identity, tool permission, autonomy limit, incident threshold, and recoverability condition bounds the workflow?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Pattern 1: Focused Analytic Reasoner: agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the agent run and assurance card fields for Pattern 1: Focused Analytic Reasoner.	Unit profile note.	Evidence artifacts include tool-allowlist record, external-memory governance boundary.
4. Challenge	Test the misconception that naming an agent pattern certifies it is safe to deploy without governance gates.	Failure-mode note.	The artifact applies the key distinction: separate agent assistance from autonomous external action.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

46.2.4.1 AGEINT Design Patterns and Archetypes instructor notes: source reasoning, review points, and studio focus

Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**. [233, 2026]; [258, 2026].

46.2.4.2 AGEINT Design Patterns and Archetypes extension exercise: peer validation and refresh trigger review

Evidence anchor. Section 46; [233, 2026].

Have learners swap artifacts and apply the **Agentic Tool-Governance Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**.

46.2.5 AGEINT Design Patterns and Archetypes knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 46; [233, 2026].

1. Explain how **Pattern 1: Focused Analytic Reasoner (source identity preserved in pattern registry) - keeps reasoning reviewable without exposing hidden reasoning or delegating action** is defined here; name the source descriptor that supports the definition.
2. Contrast **Pattern 1: Focused Analytic Reasoner** with **Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes** using the **Agentic Tool-Governance Lens** artifact fields.
3. Identify one failure mode from the **Agentic AI Governance and Tool Security** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which permission can be removed while preserving the learning objective?
5. Correct this misconception: that naming an agent pattern certifies it is safe to deploy without governance gates.

46.2.5.1 AGEINT Design Patterns and Archetypes answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Pattern 1: Focused Analytic Reasoner** without source evidence, uncertainty, or a safe transfer task.

46.3 AGEINT Design Patterns and Archetypes assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 46; [233, 2026].

46.3.1 AGEINT Design Patterns and Archetypes evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 46; [233, 2026].

46.3.2 AGEINT Design Patterns and Archetypes transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 46; [233, 2026].

46.3.2.1 AGEINT Design Patterns and Archetypes lineage and source tradition: profile, concepts, and first anchors This sits in the **Agentic AI Governance and Tool Security** lineage: delegated action under explicit authority, identity, permissions, tool boundaries, monitoring, and human escalation. [233, 2026]; [258, 2026].

46.3.2.2 AGEINT Design Patterns and Archetypes working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 46; [233, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**, with provenance and reviewability throughout.

46.3.2.3 AGEINT Design Patterns and Archetypes knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [233, 2026]; [258, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

46.3.2.4 AGEINT Design Patterns and Archetypes transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 46; [233, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**.
- **Evidence contract:** keep the **Agentic AI Governance and Tool Security** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

46.3.2.5 AGEINT Design Patterns and Archetypes profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 46; [233, 2026].

The matched profile emphasizes delegated action under explicit authority, identity, permissions, tool boundaries, monitoring, and human escalation. The method stack is AI RMF Govern-Map-Measure-Manage, least-privilege tool design, prompt-injection review, progressive deployment, and rollback drills; the local topic cluster is **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**.

46.3.3 AGEINT Design Patterns and Archetypes evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 46; [233, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Agentic AI Governance and Tool Security** profile tells reviewers what evidence is strong enough for the module artifact built around **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**.

46.3.3.1 AGEINT Design Patterns and Archetypes guide source spine: inherited keys and local citation roles Primary guide citations: [233, 2026]; [258, 2026]; [272, 2026]; [275, 2026]; [276, 2026]; [283, 2026]; [286, 2026]; [293, 2026]; [295, 2026]; [143, 2026]; [139, 2026]; [144, 2026]; [145, 2026]; [146, 2026]; [147, 2026]; [148, 2026]; [138, 2026]; [004, 2026]; [149, 2026]; [150, 2026]; [076, 2026]; [151, 2026]; [152, 2026]; [137, 2026]; [299, 2026]; [306, 2026]; [312, 2026]; [297, 2026]; [298, 2026]; [309, 2026]; [310, 2026]; [300, 2026]; [304, 2026]; [303, 2026]; [305, 2026]; [302, 2026]; [301, 2026]; [307, 2026]; [308, 2026]; [311, 2026].

46.3.3.2 AGEINT Design Patterns and Archetypes verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [233, 2026]; [258, 2026].

Tier	What counts	How it is used
Source guide	[233, 2026]; [258, 2026]; [272, 2026]; [275, 2026]; [276, 2026]; [283, 2026]; [286, 2026]; [293, 2026]; [295, 2026]; [143, 2026]; [139, 2026]; [144, 2026]; [145, 2026]; [146, 2026]; [147, 2026]; [148, 2026]; [138, 2026]; [004, 2026]; [149, 2026]; [150, 2026]; [076, 2026]; [151, 2026]; [152, 2026]; [137, 2026]; [299, 2026]; [306, 2026]; [312, 2026]; [297, 2026]; [298, 2026]; [309, 2026]; [310, 2026]; [300, 2026]; [304, 2026]; [303, 2026]; [305, 2026]; [302, 2026]; [301, 2026]; [307, 2026]; [308, 2026]; [311, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 32's source-canon section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes** and [233, 2026]; [258, 2026], but only directly verified source URLs are encoded as citations.

46.3.3.3 AGEINT Design Patterns and Archetypes intelligence practice lens: evidence artifact and safety check Practice lens: **Agentic Tool-Governance Lens** for **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**. [233, 2026]; [258, 2026].

Planning question: Which human authority, agent identity, tool permission, autonomy limit, incident threshold, and recoverability condition bounds the workflow?

Evidence artifact: agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path.

Validation rule: verify least privilege, prompt-injection exposure, provenance, observability, stop conditions, and incident-reporting triggers. Applied to **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**.

Handoff contract: export agent traces, tool calls, retrieved sources, policy decisions, and human approvals separately.

Safety check: block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions.

46.3.3.4 AGEINT Design Patterns and Archetypes runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 46; [233, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	32.99	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
AGEINT pattern registry, agent identity, and interface-contract studio	32.100	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Bounded autonomy, procurement, incident-response, and assurance studio	32.101	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Model-card, recoverability, retention, and learner-support evidence package	32.102	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 1: Focused Analytic Reasoner (source identity preserved in pattern registry) - keeps reasoning reviewable without exposing hidden reasoning or delegating action	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: single public-source report critique with provenance and uncertainty fields	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Focused Analytic Reasoner	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Pattern 2: Reflection and Bias-Check Agent (source identity preserved in pattern registry) - supports quality review and never replaces accountable human judgment	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: rubric-based critique, source-quality scoring, and trajectory validation	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: analytic-bias review over a synthetic or public-source evidence packet	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Reflection and Bias-Check Agent	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 3: Tool-Allowlist Research Assistant (source identity preserved in pattern registry) - excludes broad scraping, credentialed collection, and exposure-search tooling	module section	Source identity preserved in pattern registry with safe classroom treatment	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Safe methods: schema-bound tool calls, public-source retrieval, allowlisted connectors, and grounded summaries	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: accountable bibliography, source inventory, or standards-mapping exercise	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Tool-Allowlist Research Assistant	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 4: Governed Planner-Executor (source identity preserved in pattern registry) - plans curriculum artifacts only and does not create live operational tasking	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: milestone decomposition, approval gates, dependency checks, and rollback notes	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: classroom project plan for evidence review, policy analysis, or tabletop preparation	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Governed Planner-Executor	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 5: Parallel Source-Corroboration Agent (source identity preserved in pattern registry) - uses public or provided materials and avoids intelligence collection expansion	module section	Source identity preserved in pattern registry with safe classroom treatment	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Safe methods: bounded concurrent retrieval, deduplication, contradiction capture, and source descriptors	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: side-by-side comparison of public official, standards, and scholarly sources	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Parallel Source-Corroboration Agent	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 6: Role-Separated Review Crew (source identity preserved in pattern registry) - keeps roles educational, logged, and constrained to benign artifacts	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: planner, retriever, validator, safety reviewer, and reporter roles	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: tabletop red-team critique of an analytic memo, not an operational exercise	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Role-Separated Review Crew	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 7: Competing-Hypotheses Debate Agent (source identity preserved in pattern registry) - does not generate adversarial persuasion or policy advocacy content	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: alternative generation, evidence challenge, dissent capture, and judge rubric	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Safe defensive application: ACH-style review of a classroom claim with clearly separated evidence and judgment	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Competing-Hypotheses Debate Agent	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 8: Provenance-Bound Retrieval Operator (source identity preserved in pattern registry) - does not connect to live sensitive stores or unapproved data collections	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: curated corpus retrieval, hybrid ranking, source snippets, and citation audits	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: course-pack retrieval over provided readings, standards, and official guidance	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Provenance-Bound Retrieval Operator	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 9: Evidence-Memory State Machine (source identity preserved in pattern registry) - tracks claims and sources, not people, assets, or behavioral patterns	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: episodic note cards, retention limits, consolidation, and source change logs	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: longitudinal claim ledger for curriculum evidence and revision history	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Evidence-Memory State Machine	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 10: Permissioned Control Plane Agent (source identity preserved in pattern registry) - keeps every tool revocable, observable, and constrained to evidence-bounded actions	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Safe methods: single-interface routing, policy checks, budget limits, and audit logs	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: tool-governance demo that routes among benign summarization and validation utilities	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Permissioned Control Plane Agent	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 11: Monitoring-Governance Tabletop Agent (source identity preserved in pattern registry) - prohibits tracking real people, real targets, private forums, or infrastructure	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: synthetic event polling, threshold rationale, alert review, and escalation logging	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: accountable monitoring governance exercise over toy asset-health records	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Monitoring-Governance Tabletop Agent	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 12: Control-Coverage Critique Agent (source identity preserved in pattern registry) - does not automate exploitation, weakness discovery, or attack-chain execution	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: policy-safe scenario cards, control mapping, misuse-case review, and mitigation scoring	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: defensive tabletop review of controls against published high-level tactics	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Control-Coverage Critique Agent	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Pattern 13: Identity-and-Provenance Fiction Audit (source identity preserved in pattern registry) - prohibits impersonation, false identity creation, and operational-security support	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: synthetic persona-risk critique, provenance labeling, and consistency-error detection	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: ethics exercise that detects fabricated identity artifacts in clearly synthetic materials	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Identity-and-Provenance Fiction Audit	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 14: Source-Reliability Verification Agent (source identity preserved in pattern registry) - supports verification and does not accuse, deanonymize, or profile real people	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: corroboration, metadata review, provenance checks, and content-authenticity labels	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: public-source validation packet with uncertainty and review escalations	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Source-Reliability Verification Agent	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 15: Analyst-in-the-Loop Review Agent (source identity preserved in pattern registry) - requires accountable human review before any external communication or decision	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: interrupt gates, confidence thresholds, human approvals, and audit handoffs	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: supervised classroom analysis workflow for compliance-constrained exercises	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Analyst-in-the-Loop Review Agent	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 16: SOC Tabletop Triage Agent (source identity preserved in pattern registry) - does not run response actions, touch production systems, or publish indicators as fact	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: synthetic alert enrichment, ATT&CK mapping, severity rationale, and debrief notes	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: tier-1 incident tabletop over fabricated logs and published technique descriptions	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for SOC Tabletop Triage Agent	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 17: Software Provenance Review Agent (source identity preserved in pattern registry) - does not hunt real maintainers or produce exploitability claims without evidence	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: SBOM reading, dependency graph review, advisory matching, and integrity questions	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: defensive package-governance exercise over sample manifests and public advisories	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Software Provenance Review Agent	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 18: GEOINT Data-Quality Audit Agent (source identity preserved in pattern registry) - limits work to non-sensitive metadata quality, uncertainty notes, and synthetic location examples	module section	Source identity preserved in pattern registry with safe classroom treatment	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Safe methods: provided-image annotation, quality flags, geospatial metadata review, and caveat writing	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Safe defensive application: synthetic imagery-change exercise focused on uncertainty and data quality	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for GEOINT Data-Quality Audit Agent	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 19: Cognitive-Resilience Education Agent (source identity preserved in pattern registry) - does not design persuasion campaigns, microtargeting, or covert influence content	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: manipulation-technique labeling, transparent prebunking, and audience-harm review	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: opt-in media-literacy micro-lesson for a sample classroom scenario	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Cognitive-Resilience Education Agent	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 20: Hierarchical Curriculum Orchestrator (source identity preserved in pattern registry) - orchestrates learning artifacts only and preserves human authorization gates	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: role delegation, output aggregation, exception routing, and failure recovery drills	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: multi-domain capstone coordination across benign module artifacts	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Hierarchical Curriculum Orchestrator	module section	Source identity preserved in pattern registry with safe classroom treatment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

46.3.3.5 AGEINT Design Patterns and Archetypes reusable subsection contract: topic rows, artifacts, and safety duties Evidence anchor. Section 46; [233, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Pattern 1: Focused Analytic Reasoner (source identity preserved in pattern registry) - keeps reasoning reviewable without exposing hidden reasoning or delegating action	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: single public-source report critique with provenance and uncertainty fields	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Focused Analytic Reasoner	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 2: Reflection and Bias-Check Agent (source identity preserved in pattern registry) - supports quality review and never replaces accountable human judgment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: rubric-based critique, source-quality scoring, and trajectory validation	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: analytic-bias review over a synthetic or public-source evidence packet	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Reflection and Bias-Check Agent	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 3: Tool-Allowlist Research Assistant (source identity preserved in pattern registry) - excludes broad scraping, credentialed collection, and exposure-search tooling	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Safe methods: schema-bound tool calls, public-source retrieval, allowlisted connectors, and grounded summaries	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: accountable bibliography, source inventory, or standards-mapping exercise	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Tool-Allowlist Research Assistant	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 4: Governed Planner-Executor (source identity preserved in pattern registry) - plans curriculum artifacts only and does not create live operational tasking	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: milestone decomposition, approval gates, dependency checks, and rollback notes	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: classroom project plan for evidence review, policy analysis, or tabletop preparation	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Governed Planner-Executor	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 5: Parallel Source-Corroboration Agent (source identity preserved in pattern registry) - uses public or provided materials and avoids intelligence collection expansion	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

Lesson topic	Practice lens	Evidence artifact	Safety check
Safe methods: bounded concurrent retrieval, deduplication, contradiction capture, and source descriptors	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: side-by-side comparison of public official, standards, and scholarly sources	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Parallel Source-Corroboration Agent	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 6: Role-Separated Review Crew (source identity preserved in pattern registry) - keeps roles educational, logged, and constrained to benign artifacts	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: planner, retriever, validator, safety reviewer, and reporter roles	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: tabletop red-team critique of an analytic memo, not an operational exercise	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Role-Separated Review Crew	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 7: Competing-Hypotheses Debate Agent (source identity preserved in pattern registry) - does not generate adversarial persuasion or policy advocacy content	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: alternative generation, evidence challenge, dissent capture, and judge rubric	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: ACH-style review of a classroom claim with clearly separated evidence and judgment	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Competing-Hypotheses Debate Agent	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 8: Provenance-Bound Retrieval Operator (source identity preserved in pattern registry) - does not connect to live sensitive stores or unapproved data collections	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: curated corpus retrieval, hybrid ranking, source snippets, and citation audits	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: course-pack retrieval over provided readings, standards, and official guidance	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Provenance-Bound Retrieval Operator	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 9: Evidence-Memory State Machine (source identity preserved in pattern registry) - tracks claims and sources, not people, assets, or behavioral patterns	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: episodic note cards, retention limits, consolidation, and source change logs	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: longitudinal claim ledger for curriculum evidence and revision history	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

Lesson topic	Practice lens	Evidence artifact	Safety check
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Evidence-Memory State Machine	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 10: Permissioned Control Plane Agent (source identity preserved in pattern registry) - keeps every tool revocable, observable, and constrained to evidence-bounded actions	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: single-interface routing, policy checks, budget limits, and audit logs	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: tool-governance demo that routes among benign summarization and validation utilities	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Permissioned Control Plane Agent	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 11: Monitoring-Governance Tabletop Agent (source identity preserved in pattern registry) - prohibits tracking real people, real targets, private forums, or infrastructure	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: synthetic event polling, threshold rationale, alert review, and escalation logging	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: accountable monitoring governance exercise over toy asset-health records	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Monitoring-Governance Tabletop Agent	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 12: Control-Coverage Critique Agent (source identity preserved in pattern registry) - does not automate exploitation, weakness discovery, or attack-chain execution	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: policy-safe scenario cards, control mapping, misuse-case review, and mitigation scoring	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: defensive tabletop review of controls against published high-level tactics	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Control-Coverage Critique Agent	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 13: Identity-and-Provenance Fiction Audit (source identity preserved in pattern registry) - prohibits impersonation, false identity creation, and operational-security support	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: synthetic persona-risk critique, provenance labeling, and consistency-error detection	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: ethics exercise that detects fabricated identity artifacts in clearly synthetic materials	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Identity-and-Provenance Fiction Audit	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

Lesson topic	Practice lens	Evidence artifact	Safety check
Pattern 14: Source-Reliability Verification Agent (source identity preserved in pattern registry) - supports verification and does not accuse, deanonymize, or profile real people	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: corroboration, metadata review, provenance checks, and content-authenticity labels	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: public-source validation packet with uncertainty and review escalations	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Source-Reliability Verification Agent	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 15: Analyst-in-the-Loop Review Agent (source identity preserved in pattern registry) - requires accountable human review before any external communication or decision	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: interrupt gates, confidence thresholds, human approvals, and audit handoffs	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: supervised classroom analysis workflow for compliance-constrained exercises	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Analyst-in-the-Loop Review Agent	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 16: SOC Tabletop Triage Agent (source identity preserved in pattern registry) - does not run response actions, touch production systems, or publish indicators as fact	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: synthetic alert enrichment, ATT&CK mapping, severity rationale, and debrief notes	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: tier-1 incident tabletop over fabricated logs and published technique descriptions	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for SOC Tabletop Triage Agent	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 17: Software Provenance Review Agent (source identity preserved in pattern registry) - does not hunt real maintainers or produce exploitability claims without evidence	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: SBOM reading, dependency graph review, advisory matching, and integrity questions	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: defensive package-governance exercise over sample manifests and public advisories	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Software Provenance Review Agent	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 18: GEOINT Data-Quality Audit Agent (source identity preserved in pattern registry) - limits work to non-sensitive metadata quality, uncertainty notes, and synthetic location examples	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure

Lesson topic	Practice lens	Evidence artifact	Safety check
Safe methods: provided-image annotation, quality flags, geospatial metadata review, and caveat writing	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: synthetic imagery-change exercise focused on uncertainty and data quality	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for GEOINT Data-Quality Audit Agent	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 19: Cognitive-Resilience Education Agent (source identity preserved in pattern registry) - does not design persuasion campaigns, microtargeting, or covert influence content	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: manipulation-technique labeling, transparent prebunking, and audience-harm	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: opt-in media-literacy micro-lesson for a sample classroom scenario	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Cognitive-Resilience Education Agent	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Pattern 20: Hierarchical Curriculum Orchestrator (source identity preserved in pattern registry) - orchestrates learning artifacts only and preserves human authorization gates	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe methods: role delegation, output aggregation, exception routing, and failure recovery drills	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe defensive application: multi-domain capstone coordination across benign module artifacts	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Safe architecture artifact: diagram an allowlisted, logged, revocable workflow for Hierarchical Curriculum Orchestrator	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

46.3.3.6 AGEINT Design Patterns and Archetypes annotated source ledger: real titles and local contribution Each source cited by this **Agentic AI Governance and Tool Security** module is paired below with its real title and a one-line note on what it contributes to **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**.

Source	Cited work	What it contributes	Status
[233, 2026]	General-Purpose AI Code of Practice	An official European Commission Digital Strategy webpage documenting the General-Purpose AI Code of Practice, a voluntary guidance document helping general-purpose AI providers comply with the EU AI Act's rules on safety, transparency, and copyright. It describes an iterative drafting process involving nearly 1,000 stakeholders across four working groups, running from September 2024 through July 2025.	verified source-guide

Source	Cited work	What it contributes	Status
[258, 2026]	OpenAPI Specification	The official OpenAPI Initiative publications page, serving as a central index for the OpenAPI Specification and related standards including the Arazzo and Overlay specifications. It provides access to multiple specification versions (2.0, 3.0, 3.1, and 3.2) and their corresponding downloadable schemas identified by release date, along with a registry of extensions, formats, media types, and other resources.	verified source-guide
[272, 2026]	C2PA Specifications	The specifications hub for the C2PA (Coalition for Content Provenance and Authenticity), a standards initiative that develops technical methods for certifying the source and history of media content to counter misleading information. It publishes the core Content Credentials specification along with related material such as attestations and a soft-binding API, plus implementation, security, and user-experience guidance including for AI-generated content.	verified source-guide
[275, 2026]	Fact Sheet: New Rule on the Accessibility of Web Content and Mobile Apps Provided by State and Local Governments	A US Department of Justice fact sheet explaining the 2024 ADA Title II rule requiring state and local governments to make their web content and mobile apps accessible. It establishes WCAG 2.1 Level AA as the technical standard, applies to entities such as schools, courts, libraries, and transit agencies, and sets compliance deadlines of April 2027 for larger jurisdictions and April 2028 for smaller ones.	verified source-guide
[276, 2026]	What is a Data Protection Impact Assessment and When Is This Mandatory?	A European Data Protection Board FAQ page, part of its data protection guide for small businesses, explaining Data Protection Impact Assessments (DPIAs) and when they are mandatory. It describes a DPIA as a written assessment of the impact of a planned processing operation, required when processing poses high risks to individuals' rights.	verified source-guide
[283, 2026]	Recommendation of the Council on Open Government	An OECD legal instrument document reproducing the Recommendation of the Council on Open Government (OECD/LEGAL/0438), adopted on 14 December 2017. It defines open government as a culture of governance promoting transparency, integrity, accountability, and stakeholder participation in support of democracy and inclusive growth.	verified source-guide
[286, 2026]	Model Cards for Model Reporting	The arXiv abstract for "Model Cards for Model Reporting" (2018) by Mitchell, Wu, Zaldivar, and colleagues, which introduces a framework for transparent documentation of machine learning models. Model cards are short accompanying documents that report a model's benchmarked performance across varied conditions, including different cultural, demographic, and phenotypic groups, along with intended use, evaluation methodology, and deployment considerations.	verified source-guide

Source	Cited work	What it contributes	Status
[293, 2026]	Inventory of NARA Artificial Intelligence (AI) Use Cases	The National Archives and Records Administration (NARA) official inventory of its artificial intelligence use cases, documenting 14 projects across deployed, pilot, and planned stages. Deployed efforts include workplace productivity tools, automated tagging for museum experiences, and historical record retrieval, while pilots cover PII detection and redaction, semantic search, and metadata generation, and planned work targets FOIA processing and public search.	verified source-guide
[295, 2026]	M-25-22: Driving Efficient Acquisition of Artificial Intelligence in Government	OMB Memorandum M-25-22 (April 3, 2025), Driving Efficient Acquisition of Artificial Intelligence in Government, issued under Executive Order 13960 and related directives. It provides guidance to federal agencies for acquiring effective and trustworthy AI in a timely, cost-effective manner, and rescinds and replaces earlier memorandum M-24-18.	verified source-guide
[143, 2026]	Agentic AI Architectures And Design Patterns / by Anil Jain	A Medium article by Anil Jain (2025) surveying agentic AI system architectures and design patterns. It defines agentic AI as systems capable of independent decision-making, reviews frameworks such as LangChain, LlamaIndex, and AutoGen, and describes five system components: perception, decision-making, action, memory, and communication.	verified practitioner context; secondary evidence only
[139, 2026]	Agentic AI Design Patterns by Andrew Ng	A LinkedIn post by Aishwarya Srinivasan discussing agentic AI design patterns for building production-grade AI agents.	verified practitioner context; secondary evidence only
[144, 2026]	Agentic AI patterns and workflows on AWS	An AWS Prescriptive Guidance document (July 2025) introducing agentic AI patterns and workflows. It presents reusable design templates for building AI agent systems that operate with autonomy while remaining controllable and aligned with goals, aimed at architects, developers, and product leaders.	verified practitioner context; secondary evidence only
[145, 2026]	A Scalable Design Pattern for Agentic AI Systems	This is an arXiv research paper by Sivasathivel Kandasamy titled "Control Plane as a Tool: A Scalable Design Pattern for Agentic AI Systems." It proposes an architectural pattern in which AI agents interact with a single control-plane interface that handles tool routing and selection, rather than exposing many tools directly.	verified source-guide
[146, 2026]	Agentic AI Frameworks: Key Components & Top 8 Options in 2026	An Exabeam explainer describing agentic AI frameworks as software toolkits that provide pre-built components and architectures for building autonomous AI agents. It outlines core elements such as agent coordination, tool integration, memory management, workflow definition, and deployment monitoring, and reviews eight frameworks including LangGraph, AutoGen, CrewAI, LlamaIndex, Haystack, DSPy, and Semantic Kernel.	verified source-guide

Source	Cited work	What it contributes	Status
[147, 2026]	Agent Framework Security	Security analysis of major AI agent frameworks including LangChain, CrewAI, AutoGen, Semantic.	original practitioner context; secondary evidence only
[148, 2026]	How Riverside Research Advances Agentic AI for National Security	This article by Riverside Research traces AI's evolution from large language models through retrieval-augmented systems, single-task agents, collaborative agentic systems, and toward emergent multi-agent autonomy capable of managing surveillance and decision support at operational speed.	verified source-guide
[138, 2026]	Agentic Artificial Intelligence (AI): Architectures, Taxonomies	An arXiv survey paper on agentic AI examining the shift from generative systems to autonomous agents that perceive, reason, plan, and act. It proposes a unified taxonomy decomposing LLM-based agents into six dimensions: core components, cognitive architecture, learning paradigms, multi-agent systems, environments and domains, and evaluation and safety.	verified source-guide
[004, 2026]	AI Won't Replace Spies—It Will Make Them More Powerful Than Ever	Tom Mulligan argues that artificial intelligence will enhance rather than replace human intelligence professionals, contending that the future of intelligence lies in human-machine collaboration. He maintains that uniquely human qualities such as intuition, experience, and independent judgment become more valuable as adversaries gain access to the same AI tools.	verified source-guide
[149, 2026]	Cited source (see bibliography)	A 2025 blog article from Simbian AI explaining the application of agentic AI to security operations centers. It describes an architecture organized into perception, cognitive, and action modules, and a coordinated framework of specialized agents for tasks such as alert triage, threat investigation, and vulnerability management.	verified source-guide
[150, 2026]	The Right Role for Agentic AI in Security Operations	An article from Cybersecurity Tribe examining where autonomous AI should and should not operate within security operations, drawing on survey data and commentary from numerous security experts. It identifies high-volume, repetitive tasks such as alert triage and policy validation as well suited to automation, while warning against autonomous handling of irreversible or high-impact decisions affecting infrastructure and access.	verified source-guide
[076, 2026]	XZ Utils backdoor	In early 2024, a malicious backdoor was discovered embedded in XZ Utils, a widely used compression library in Linux distributions, designed to enable unauthorized remote code execution via OpenSSH using an Ed448 private key. The perpetrator, operating under the pseudonym Jia Tan, spent over two years building trust as a contributor before inserting the exploit, which received a maximum CVSS score of 10.0.	verified source-guide context; do not use as primary analytic support

Source	Cited work	What it contributes	Status
[151, 2026]	A Practical Guide to Prebunking Misinformation - Inoculation Science	A practitioner guide from Inoculation Science explaining prebunking as a proactive strategy to build preemptive resilience to misinformation. Grounded in inoculation theory, it describes how exposing people to weakened forms of manipulative content can help them develop resistance before they encounter it in the wild.	verified source-guide
[152, 2026]	Social media experiment reveals potential to 'inoculate' millions	A University of Cambridge news article describing a large study, conducted with Bristol University and Google's Jigsaw, testing whether short animated videos can help people resist online manipulation. The 90-second clips expose common manipulation techniques such as scapegoating, false dichotomies, and emotionally manipulative language, an approach the researchers call prebunking.	verified source-guide
[137, 2026]	[2601.12560] Agentic Artificial Intelligence (AI)	An arXiv paper surveying the shift from passive language models to Agentic AI, where large language models act as cognitive controllers that combine memory, tool use, and environmental feedback to pursue extended goals. It proposes a unified taxonomy organizing agent systems into six components: perception, brain, planning, action, tool use, and collaboration.	verified source-guide
[299, 2026]	Model Context Protocol Specification	The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation).	verified source-guide context; use pinned MCP anchor for normative claims
[306, 2026]	Artificial Intelligence	Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support.	original source-guide
[312, 2026]	Guide on the Use of Agentic Artificial Intelligence	Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support.	original source-guide
[297, 2026]	Intelligence Community Directive 203: Analytic Standards	Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products.	original source-guide
[298, 2026]	Intelligence Community Directives	Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations.	original source-guide

Source	Cited work	What it contributes	Status
[309, 2026]	STIX Version 2.1	An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection.	verified source-guide

The remaining 10 cited source(s) appear in the bibliography appendix with the same verification metadata.

Where this sits. This module's overview is Section 46; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

46.3.4 AGEINT Design Patterns and Archetypes governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 46; [233, 2026].

46.3.5 AGEINT Design Patterns and Archetypes analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 32's governance-boundary section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **Agentic AI Governance and Tool Security** for **Pattern 1: Focused Analytic Reasoner (source identity preserved in pattern registry) - keeps reasoning reviewable without exposing hidden reasoning or delegating action; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**. [233, 2026]; [258, 2026].

Curriculum topic spine: Pattern 1: Focused Analytic Reasoner (source identity preserved in pattern registry) - keeps reasoning reviewable without exposing hidden reasoning or delegating action, **Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**, **Safe defensive application: single public-source report critique with provenance and uncertainty fields**. **Verified anchor cluster:** [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]; [Community, 2020b]; [Community, 2020a]; [of the Director of National Intelligence, 2025b].

Conceptual depth: delegated action under explicit authority, identity, permissions, tool boundaries, monitoring, and human escalation.

Method stack: AI RMF Govern-Map-Measure-Manage, least-privilege tool design, prompt-injection review, progressive deployment, and rollback drills.

Composability contract: agents, tools, credentials, memory, retrieval stores, policies, and logs remain separately inspectable and revocable components.

Known failure modes: excessive agency, shadow tools, indirect prompt injection, memory poisoning, confused authority, and unbounded action chains.

Defensive boundary: agentic workflows stay synthetic, owned-lab, supervised, logged, rate-limited, and reversible unless a lawful production authority exists. Applied to **Pattern 1: Focused Analytic Reasoner (source identity preserved in pattern registry) - keeps reasoning reviewable without exposing hidden reasoning or delegating action; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**.

Anchor	Why it matters here
[OECD, 2026a]	Official OECD conceptual foundation for agentic AI. Checked as of 2026-05-21; role: source_quality_anchor.
[of Canada Secretariat, 2026a]	Government of Canada guide for accountable public-sector use of agentic AI, including governance, risk, transparency, testing, monitoring, and human oversight considerations. Checked as of 2026-05-24; role: curriculum_anchor.
[of Standards and Technology, 2023]	Official NIST.AI.100-1 risk-management framework. Checked as of 2026-05-21; role: source_quality_anchor.
[of Standards and Technology, 2024d]	Official NIST AI 600-1 generative AI profile. Checked as of 2026-05-21; role: source_quality_anchor.
[Community, 2020b]	Official IC principles for lawful, accountable, objective, human-centered, secure, resilient, and science-informed AI. Checked as of 2026-05-21; role: curriculum_anchor.
[Community, 2020a]	Official IC framework for AI goals, authorities, human judgment, bias mitigation, testing, documentation, explainability, and review. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2025b]	Official IC AI governance directive covering CAIO roles, oversight, interoperability, civil-liberties review, training data, and impact assessment. Checked as of 2026-05-21; role: curriculum_anchor.

46.3.5.1 AGEINT Design Patterns and Archetypes evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **Agentic AI Governance and Tool Security** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [233, 2026]; [258, 2026].

46.3.6 AGEINT Design Patterns and Archetypes agentic boundary: assist, approve, block, and record

Evidence anchor. Section 46; [233, 2026].

AGEINT translation is bounded by the **Agentic AI Governance and Tool Security** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**.

46.3.6.1 AGEINT Design Patterns and Archetypes permitted defensive utility: curriculum uses and safe outputs Evidence anchor.

Section 46; [233, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**.

46.3.6.2 AGEINT Design Patterns and Archetypes excluded operational boundary: blocked actions and stop rules Evidence anchor.

Section 46; [233, 2026].

Raw design-pattern motifs are transformed into accountable tabletop, audit, provenance, control-coverage, and governance exercises. The module preserves source identity in the pattern registry while rewriting methods, applications, and architecture artifacts for **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes** into evidence-bounded curriculum treatments.

46.3.7 AGEINT Design Patterns and Archetypes governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 46; [233, 2026].
Governance is practiced as a gate on the **Agentic AI Governance and Tool Security** lane. Learners use the **Agentic Tool-Governance Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**.

46.3.7.1 AGEINT Design Patterns and Archetypes governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [233, 2026]; [258, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Agentic AI Governance and Tool Security** failure modes and the **Agentic Tool-Governance Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

46.3.7.2 AGEINT Design Patterns and Archetypes evidence package handoff: appendices, records, and reuse

Evidence anchor. Section 46; [233, 2026].
Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Agentic Tool-Governance Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**.

46.3.7.3 AGEINT Design Patterns and Archetypes current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**. [233, 2026]; [258, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_oecd_agentic_ai` for **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**?	The Agentic AI Landscape and Its Conceptual Foundations; lane `source_quality_spine`; checked 2026-05-21.	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path; Official OECD conceptual foundation for agentic AI.
What does the module inherit from `official_canada_agentic_ai_guide` for **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**?	Guide on the Use of Agentic Artificial Intelligence; lane `public_sector_agentic_ai`; checked 2026-05-24.	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path; bounded-autonomy run card, recoverability review, approval threshold, monitoring evidence, and public-sector service assurance
What does the module inherit from `official_nist_ai_rmf` for **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**?	Artificial Intelligence Risk Management Framework (AI RMF 1.0); lane `source_quality_spine`; checked 2026-05-21.	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path; Official NIST.AI.100-1 risk-management framework.
What does the module inherit from `official_nist_ai_600_1` for **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**?	Artificial Intelligence Risk Management Framework: Generative AI Profile; lane `source_quality_spine`; checked 2026-05-21.	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path; Official NIST AI 600-1 generative AI profile.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 46; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

46.3.8 AGEINT Design Patterns and Archetypes assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 46; [233, 2026].

46.3.9 AGEINT Design Patterns and Archetypes assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 46; [233, 2026].

46.3.9.1 AGEINT Design Patterns and Archetypes capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**.
Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes** and [233, 2026]; [258, 2026].

46.3.9.2 AGEINT Design Patterns and Archetypes instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes** and [233, 2026]; [258, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

46.3.9.3 AGEINT Design Patterns and Archetypes assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Pattern 1: Focused Analytic Reasoner (source identity preserved in pattern registry) - keeps reasoning reviewable without exposing hidden reasoning or delegating action	Completed **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes	Completed **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Safe defensive application: single public-source report critique with provenance and uncertainty fields	Completed **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

46.3.10 AGEINT Design Patterns and Archetypes refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [233, 2026]; [258, 2026] and **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**.

46.3.10.1 AGEINT Design Patterns and Archetypes refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**. The local signals begin with [233, 2026]; [258, 2026].

46.3.10.2 AGEINT Design Patterns and Archetypes claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**, and the source spine for these checks begins with [233, 2026]; [258, 2026].

46.3.11 AGEINT Design Patterns and Archetypes reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [233, 2026]; [258, 2026].
Triangulation anchors. In module 32's review-checklist section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes**. [233, 2026]; [258, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.

- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

46.3.12 AGEINT Design Patterns and Archetypes learning-path links: module map, overview, and curriculum atlas

Use the cross-links below to place **Pattern 1: Focused Analytic Reasoner; Safe methods: bounded source reading, explicit assumptions, self-critique, and confidence notes** in the wider unit: the orientation sets the frame, the parent unit supplies the shared safety posture, and the neighbouring modules show what evidence enters and leaves. Lead sources: [233, 2026]; [258, 2026].

Section 2, Section 44, Section 45, Section 47

47 AGEINT Frameworks and Infrastructure

47.0.1 AGEINT Frameworks and Infrastructure figures and course links: visual evidence, source flow, and navigation

The module uses Figure 91 and Figure 85 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 44, Section 46, Section 48.
This module teaches the **Agentic AI Governance and Tool Security** lane through a bounded, source-backed coursebook chapter. [255, 2026]; [256, 2026].

47.1 Agentic AI Governance and Tool Security frame for AGEINT Frameworks and Infrastructure: source context, topic focus, and reader task

Evidence anchor. Section 47; [255, 2026].

47.1.1 AGEINT Frameworks and Infrastructure orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 47; [255, 2026].

47.1.2 AGEINT Frameworks and Infrastructure conceptual primer: source context, core model, and reader task

This chapter teaches agentic AI as delegated action under control: identity, authority, tool permissions, memory, logs, stop conditions, and recoverability define what an agent may do. The chapter uses **Agentic Tool-Governance Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**.
The central distinction is to separate agent assistance from autonomous external action. Core topics include **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language; LangGraph: Stateful, Cyclical Agentic Workflows**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [255, 2026]; [256, 2026].
Learners move from vocabulary and the **Agentic Tool-Governance Lens** distinction through topic lessons on **LangChain/LangGraph: State Machine Orchestration** with evidence and misconception checks, then assemble an **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** with safety and rights gates.

47.1.3 AGEINT Frameworks and Infrastructure learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 47; [255, 2026].

- Connect **LangChain/LangGraph: State Machine Orchestration and LCEL: LangChain Expression Language** to **Agentic AI Governance and Tool Security** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build an **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate agent assistance from autonomous external action; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as excessive agency, shadow tools, indirect prompt injection, memory poisoning, confused authority, and unbounded action chains, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: agentic workflows stay synthetic, owned-lab, supervised, logged, rate-limited, and reversible unless a lawful production authority exists.

47.1.4 AGEINT Frameworks and Infrastructure core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 47; [255, 2026].

Term	Working definition
Agent identity	the named software actor, role, and authorization context for a run
Tool allowlist	the bounded set of actions the agent may request
Delegation	the handoff of a task under explicit human authority and review
Bounded autonomy	the documented ceiling on what an agent may decide or request without review
Recoverability	the path back to a known-safe state after a bad output or action request
AI incident	a logged event where an AI system creates or plausibly creates harm or loss of control
Prompt injection	untrusted content that attempts to override instructions or authority boundaries
Pattern registry	the catalog of approved agent behaviors, prompts, and evaluation hooks
Adversarial eval	structured tests that probe agent misuse, injection, and over-delegation before release
LangChain/LangGraph: State Machine Orchestration	Key terms: LangChain, LangGraph, State.
LCEL: LangChain Expression Language	Key terms: LCEL, LangChain, Expression.

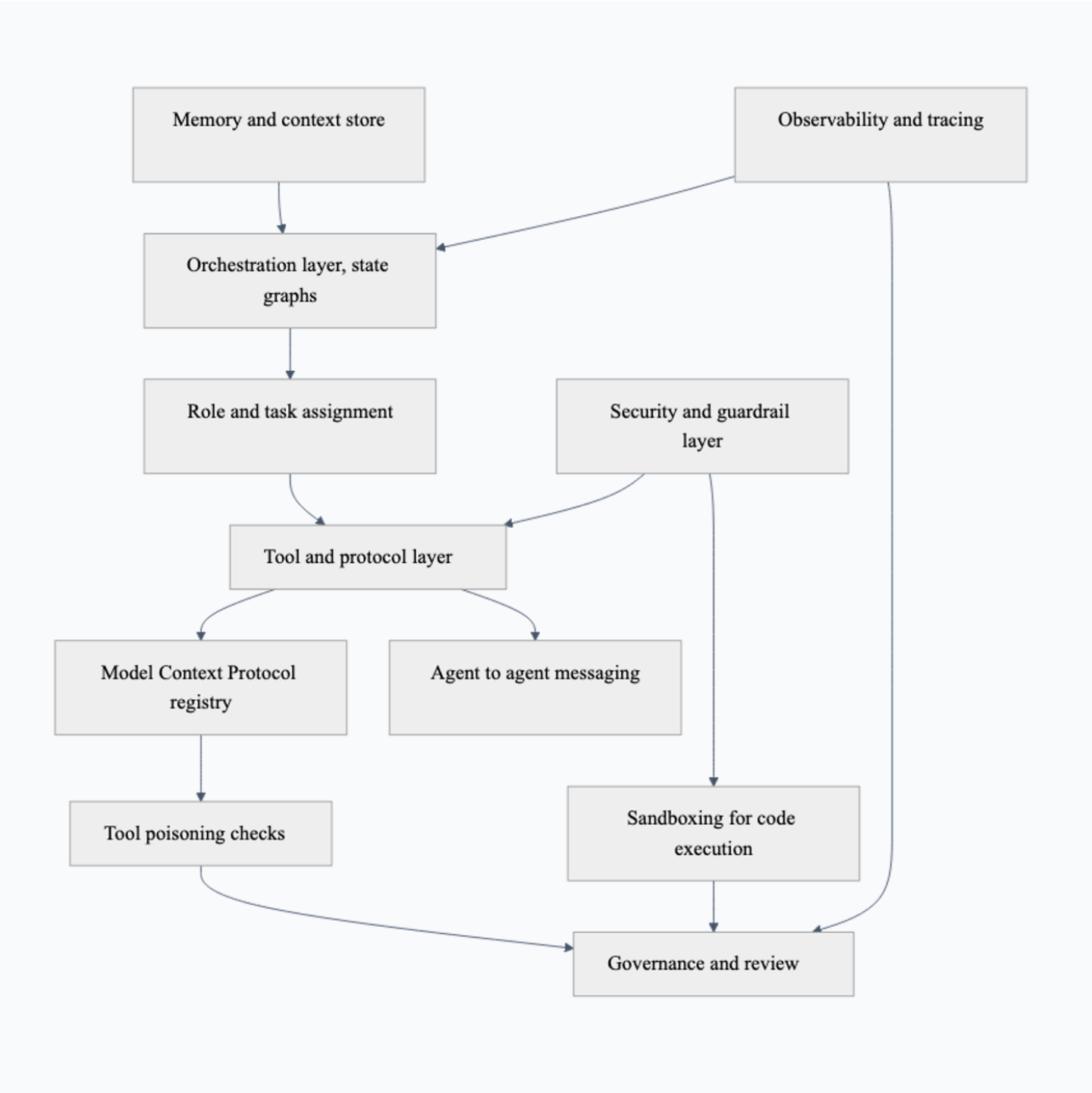


Figure 91: A layered map of agentic infrastructure showing how orchestration, tool protocols, memory, and security guardrails fit together for governed intelligence workflows. Its reader value is to make Orchestration layer, state graphs, Role and task assignment, Tool and protocol layer, and Model Context Protocol registry visible at a glance, with the ageint agentic intelligence / ageint frameworks and infrastructure section as the source section and defensive review as the boundary.

47.2 Agentic Tool-Governance Lens path for AGEINT Frameworks and Infrastructure: lesson cluster, safe artifact, and review

Evidence anchor. Section 47; [255, 2026].

47.2.1 AGEINT Frameworks and Infrastructure practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 47; [255, 2026].

47.2.2 AGEINT Frameworks and Infrastructure topic lessons: source-backed concepts and transfer tasks

This module builds agentic AI as delegated action under control: identity, authority, tool permissions, memory, logs, stop conditions, and recoverability define what an agent may do. The sequence opens with **LangChain/LangGraph: State Machine Orchestration**, **LCEL: LangChain Expression Language**, **LangGraph: Stateful, Cyclical Agentic Workflows** and applies the **Agentic Tool-Governance Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 85; module overview Section 47; curriculum atlas Section 2.

Triangulation anchors. In module 33's topic-lessons section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

47.2.2.1 Lesson 1: LangChain/LangGraph: State Machine Orchestration

Concept. LangChain/LangGraph: State Machine Orchestration documents workflow stages with inputs, transforms, reviewers, and blocked actions at each handoff.

Why it matters. LangChain/LangGraph connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. LangChain/LangGraph: State Machine Orchestration rests on [147, 2026] and [153, 2026]. The lead source's own note reads: Security analysis of major AI agent frameworks including LangChain, CrewAI, AutoGen, Semantic. Use them for pinning down the scope of **LangChain/LangGraph: State Machine Orchestration**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **LangChain/LangGraph**, reason from the sources cited in this row. [147, 2026] Security analysis of major AI agent frameworks including LangChain, CrewAI, AutoGen, Semantic. [153, 2026] The second half of the framework highlights common agentic frameworks. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **LangChain/LangGraph**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **LangChain/LangGraph**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **LangChain/LangGraph** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **LangChain/LangGraph**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **LangChain/LangGraph** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

47.2.2.2 Lesson 2: LCEL: LangChain Expression Language

Concept. LCEL: LangChain Expression Language evaluates agent frameworks by logging, tool allowlists, human approval, and blocked external actions—not production deployment recipes.

Why it matters. Without explicit treatment of **LCEL: LangChain Expression Language**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. LCEL: LangChain Expression Language rests on [299, 2026], [306, 2026], and [312, 2026]. The lead source's own note reads: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for fixing what **LCEL: LangChain Expression Language** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **LCEL: LangChain Expression Language** in the evidence the row cites. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **LCEL**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **LCEL**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **LCEL: LangChain Expression Language** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **LCEL: LangChain Expression Language**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **LCEL: LangChain Expression Language** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

47.2.2.3 Lesson 3: LangGraph: Stateful, Cyclical Agentic Workflows

Concept. LangGraph: Stateful, Cyclical Agentic Workflows evaluates agent frameworks by logging, tool allowlists, human approval, and blocked external actions—not production deployment recipes.

Why it matters. Analysts use **LangGraph: Stateful, Cyclical Agentic Workflows** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that treating pattern names as deployment playbooks would otherwise hide, and the reviewer accountable for challenge.

Source support. LangGraph: Stateful, Cyclical Agentic Workflows rests on [299, 2026], [306, 2026], and [312, 2026]. Its anchor reference records: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for fixing what **LangGraph: Stateful, Cyclical Agentic Workflows** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **LangGraph: Stateful, Cyclical Agentic Workflows**, work from the cited evidence behind this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data

sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **LangGraph**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **LangGraph**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **LangGraph: Stateful, Cyclical Agentic Workflows** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **LangGraph: Stateful, Cyclical Agentic Workflows**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **LangGraph: Stateful, Cyclical Agentic Workflows** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

47.2.2.4 Lesson 4: LangSmith: Observability and Tracing

Concept. LangSmith: Observability and Tracing evaluates agent frameworks by logging, tool allowlists, human approval, and blocked external actions—not production deployment recipes.

Why it matters. LangSmith: Observability and Tracing matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; treating pattern names as deployment playbooks is a common failure.

Source support. LangSmith: Observability and Tracing rests on [299, 2026], [306, 2026], and [312, 2026]. The lead source's own note reads: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for pinning down the scope of **LangSmith: Observability and Tracing**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **LangSmith: Observability and Tracing**, reason from the sources cited in this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **LangSmith**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **LangSmith**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **LangSmith: Observability and Tracing** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **LangSmith: Observability and Tracing**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **LangSmith: Observability and Tracing** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

47.2.2.5 Lesson 5: CrewAI: Role-Based Multi-Agent Collaboration

Concept. CrewAI: Role-Based Multi-Agent Collaboration treats agents as software actors with explicit permissions, logs, stop conditions, and human approval—not autonomous decision makers.

Why it matters. CrewAI: Role-Based Multi-Agent Collaboration connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. CrewAI: Role-Based Multi-Agent Collaboration rests on [154, 2026] and [153, 2026]. The lead source's own note reads: The homepage of CrewAI, a commercial platform for building, deploying, and managing AI agents at scale for enterprises. Use them for fixing what **CrewAI: Role-Based Multi-Agent Collaboration** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **CrewAI: Role-Based Multi-Agent Collaboration** against the works cited for this row. [154, 2026] The homepage of CrewAI, a commercial platform for building, deploying, and managing AI agents at scale for enterprises. It presents the product as covering the full lifecycle from identifying automation opportunities to launching and optimizing multi-agent workflows while maintaining enterprise-level control. [153, 2026] The second half of the framework highlights common agentic frameworks. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **CrewAI**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **CrewAI**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **CrewAI: Role-Based Multi-Agent Collaboration** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **CrewAI: Role-Based Multi-Agent Collaboration**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **CrewAI: Role-Based Multi-Agent Collaboration** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

47.2.2.6 Lesson 6: Crew, Agent, Task, and Process Objects

Concept. Crew, Agent, Task, and Process Objects treats agents as software actors with explicit permissions, logs, stop conditions, and human approval—not autonomous decision makers.

Why it matters. Without explicit treatment of **Crew, Agent, Task, and Process Objects**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Crew, Agent, Task, and Process Objects rests on [299, 2026], [306, 2026], and [312, 2026]. Its anchor reference records: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for the working definition that **Crew, Agent, Task, and Process Objects** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Crew, Agent, Task, and Process Objects** in the evidence the row cites. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector

agent governance and accountability source support. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Crew, Agent, Task, and Process Objects**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Crew Agent Task and Process**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape this subject work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Crew, Agent, Task, and Process Objects**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Crew, Agent, Task, and Process Objects** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

47.2.2.7 Lesson 7: Sequential, Parallel, and Hierarchical Process Modes

Concept. Sequential, Parallel, and Hierarchical Process Modes uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. Analysts use **Sequential, Parallel, and Hierarchical Process Modes** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that treating pattern names as deployment playbooks would otherwise hide, and the reviewer accountable for challenge.

Source support. Sequential, Parallel, and Hierarchical Process Modes rests on [299, 2026], [306, 2026], and [312, 2026]. The lead source's own note reads: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for the working definition that **Sequential, Parallel, and Hierarchical Process Modes** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **Sequential, Parallel, and Hierarchical Process Modes** against the works cited for this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Sequential, Parallel, and Hierarchical Process Modes**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Sequential Parallel and Hierarchical Process**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape this subject work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Sequential, Parallel, and Hierarchical Process Modes**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Sequential, Parallel, and Hierarchical Process Modes** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

47.2.2.8 Lesson 8: Built-in Tool Ecosystem

Concept. Built-in Tool Ecosystem uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. Without explicit treatment of **Built-in Tool Ecosystem**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Built-in Tool Ecosystem rests on [299, 2026], [306, 2026], and [312, 2026]. The lead source's own note reads: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for the working definition that **Built-in Tool Ecosystem** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **Built-in Tool Ecosystem** against the works cited for this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. Build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Built-in Tool Ecosystem**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape this subject work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Built-in Tool Ecosystem**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Built-in Tool Ecosystem** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

47.2.2.9 Lesson 9: AutoGen (Microsoft): Multi-Agent Conversation Patterns

Concept. AutoGen (Microsoft): Multi-Agent Conversation Patterns treats agents as software actors with explicit permissions, logs, stop conditions, and human approval—not autonomous decision makers.

Why it matters. AutoGen (Microsoft) connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. AutoGen (Microsoft): Multi-Agent Conversation Patterns rests on [147, 2026] and [153, 2026]. The most specific cited work observes: Security analysis of major AI agent frameworks including LangChain, CrewAI, AutoGen, Semantic. Use them for the working definition that **AutoGen (Microsoft): Multi-Agent Conversation Patterns** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **AutoGen (Microsoft)** against the works cited for this row. [147, 2026] Security analysis of major AI agent frameworks including LangChain, CrewAI, AutoGen, Semantic. [153, 2026] The second half of the framework highlights common agentic frameworks. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **AutoGen (Microsoft)**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **AutoGen**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape

AutoGen (Microsoft) work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **AutoGen (Microsoft)**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **AutoGen (Microsoft)** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

47.2.2.10 Lesson 10: AssistantAgent and UserProxyAgent Pattern

Concept. AssistantAgent and UserProxyAgent Pattern uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. Analysts use **AssistantAgent and UserProxyAgent Pattern** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that treating pattern names as deployment playbooks would otherwise hide, and the reviewer accountable for challenge.

Source support. AssistantAgent and UserProxyAgent Pattern rests on [299, 2026], [306, 2026], and [312, 2026]. Its anchor reference records: It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). Use them for fixing what **AssistantAgent and UserProxyAgent Pattern** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **AssistantAgent and UserProxyAgent Pattern**, work from the cited evidence behind this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. Build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **AssistantAgent and UserProxyAgent Pattern**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape this subject work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **AssistantAgent and UserProxyAgent Pattern**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **AssistantAgent and UserProxyAgent Pattern** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

47.2.2.11 Lesson 11: GroupChat with RoundRobin and AutoSelect Managers

Concept. GroupChat with RoundRobin and AutoSelect Managers uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. Without explicit treatment of **GroupChat with RoundRobin and AutoSelect Managers**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. GroupChat with RoundRobin and AutoSelect Managers rests on [299, 2026], [306, 2026], and [312, 2026]. The closest source to this row notes: It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). Use them for fixing what **GroupChat with RoundRobin and AutoSelect Managers** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **GroupChat with RoundRobin and AutoSelect Managers**, reason from the sources cited in this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **GroupChat with RoundRobin and AutoSelect Managers**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **GroupChat with RoundRobin and AutoSelect**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape this subject work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **GroupChat with RoundRobin and AutoSelect Managers**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **GroupChat with RoundRobin and AutoSelect Managers** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

47.2.2.12 Lesson 12: Agentic cyber-misuse control review using sample prompt records, fabricated logs, and deny-by-default tool policies

Concept. Agentic cyber-misuse control review using sample prompt records, fabricated logs, and deny-by-default tool policies treats the topic as a misuse-case control problem: identify the agent permission, prompt path, tool boundary, and blocked outcome.

Why it matters. Analysts use **Agentic cyber-misuse control review** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that treating misuse taxonomy as tool permission would otherwise hide, and the reviewer accountable for challenge.

Source support. Agentic cyber-misuse control review using sample prompt records, fabricated logs, and deny-by-default tool policies rests on [147, 2026]. The lead source's own note reads: Security analysis of major AI agent frameworks including LangChain, CrewAI, AutoGen, Semantic. Use it for pinning down the scope of **Agentic cyber-misuse control review using sample prompt records, fabricated logs, and deny-by-default tool policies**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **Agentic cyber-misuse control review** against the works cited for this row. [147, 2026] Security analysis of major AI agent frameworks including LangChain, CrewAI, AutoGen, Semantic. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Agentic cyber-misuse control review**, build a blocked-request control card with tool permission, unsafe outcome, deny rule, log evidence, and reviewer disposition. Shape **Agentic cyber-misuse control review** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Agentic cyber-misuse control review**: that a misuse taxonomy describing what an autonomous agent could do is permission or a recipe to make it do so.

Transfer task. Reuse the **Agentic cyber-misuse control review** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

47.2.2.13 Lesson 13: Semantic Kernel: Enterprise AI Orchestration

Concept. Semantic Kernel: Enterprise AI Orchestration documents workflow stages with inputs, transforms, reviewers, and blocked actions at each handoff.

Why it matters. Semantic Kernel matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; treating pattern names as deployment playbooks is a common failure.

Source support. Semantic Kernel: Enterprise AI Orchestration rests on [147, 2026]. The lead source's own note reads: Security analysis of major AI agent frameworks including LangChain, CrewAI, AutoGen, Semantic. Use it for pinning down the scope of **Semantic Kernel: Enterprise AI Orchestration**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Semantic Kernel** in the evidence the row cites. [147, 2026] Security analysis of major AI agent frameworks including LangChain, CrewAI, AutoGen, Semantic. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Semantic Kernel**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Semantic Kernel**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Semantic Kernel** work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Semantic Kernel**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Semantic Kernel** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

47.2.2.14 Lesson 14: AWS Agentic Patterns: Production Architecture Guide

Concept. AWS Agentic Patterns: Production Architecture Guide uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. AWS Agentic Patterns: Production Architecture Guide connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. AWS Agentic Patterns: Production Architecture Guide rests on [144, 2026]. The lead source's own note reads: An AWS Prescriptive Guidance document (July 2025) introducing agentic AI patterns and workflows. Use it for the working definition that **AWS Agentic Patterns: Production Architecture Guide** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **AWS Agentic Patterns: Production Architecture Guide** in the evidence the row cites. [144, 2026] An AWS Prescriptive Guidance document (July 2025) introducing agentic AI patterns and workflows. It presents reusable design templates for building AI agent systems that operate with autonomy while remaining controllable and aligned with goals, aimed at architects, developers, and product leaders. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **AWS Agentic Patterns**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **AWS Agentic Patterns**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **AWS Agentic Patterns: Production Architecture Guide** work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **AWS Agentic Patterns: Production Architecture Guide**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **AWS Agentic Patterns: Production Architecture Guide** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

47.2.2.15 Lesson 15: Basic Reasoning Agents

Concept. Basic Reasoning Agents connects cognitive science claims to analytic bias literacy: what the brain prioritizes, what it misses, and how review compensates.

Why it matters. Basic Reasoning Agents matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; treating pattern names as deployment playbooks is a common failure.

Source support. Basic Reasoning Agents rests on [299, 2026], [306, 2026], and [312, 2026]. The closest source to this row notes: It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). Use them for the working definition that **Basic Reasoning Agents** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Basic Reasoning Agents** in the evidence the row cites. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. Build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Basic Reasoning Agents**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape this subject work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Basic Reasoning Agents**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Basic Reasoning Agents** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

47.2.2.16 Lesson 16: Tool-Based Agents (Function Calling and MCP Servers)

Concept. Tool-Based Agents (Function Calling and MCP Servers) evaluates tool protocols by allowlists, logging, provenance of retrieved content, and deny-by-default policies.

Why it matters. Tool-Based Agents (Function Calling and MCP Servers) connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Tool-Based Agents (Function Calling and MCP Servers) rests on [299, 2026], [306, 2026], and [312, 2026]. The lead source's own note reads: It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). Use them for the working definition that **Tool-Based Agents (Function Calling and MCP Servers)** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Tool-Based Agents (Function Calling and MCP Servers)**, reason from the sources cited in this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Tool-Based Agents (Function Calling and MCP Servers)**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Tool-Based Agents**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape this subject work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Tool-Based Agents (Function Calling and MCP Servers)**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Tool-Based Agents (Function Calling and MCP Servers)** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

47.2.2.17 Lesson 17: Computer-Use Agents

Concept. Computer-Use Agents uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. Computer-Use Agents matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; treating pattern names as deployment playbooks is a common failure.

Source support. Computer-Use Agents rests on [299, 2026], [306, 2026], and [312, 2026]. The lead source's own note reads: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for fixing what **Computer-Use Agents** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Computer-Use Agents**, reason from the sources cited in this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. Build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Computer-Use Agents**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape this subject work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Computer-Use Agents**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Computer-Use Agents** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

47.2.2.18 Lesson 18: Coding Agents

Concept. Coding Agents uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. Analysts use **Coding Agents** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that treating pattern names as deployment playbooks would otherwise hide, and the reviewer accountable for challenge.

Source support. Coding Agents rests on [299, 2026], [306, 2026], and [312, 2026]. The lead source's own note reads: It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). Use them for the working definition that **Coding Agents** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Coding Agents** in the evidence the row cites. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. Build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Coding Agents**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape this subject work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Coding Agents**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Coding Agents** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

47.2.2.19 Lesson 19: Speech-to-Speech Agents

Concept. Speech-to-Speech Agents uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. Without explicit treatment of **Speech-to-Speech Agents**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Speech-to-Speech Agents rests on [299, 2026], [306, 2026], and [312, 2026]. The closest source to this row notes: It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots,

elicitation). Use them for pinning down the scope of **Speech-to-Speech Agents**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Speech-to-Speech Agents**, reason from the sources cited in this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. Build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Speech-to-Speech Agents**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape this subject work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Speech-to-Speech Agents**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Speech-to-Speech Agents** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

47.2.2.20 Lesson 20: Orchestration Patterns: Supervisor, Parallel, Subgraph Concept. Orchestration Patterns: Supervisor, Parallel, Subgraph documents workflow stages with inputs, transforms, reviewers, and blocked actions at each handoff.

Why it matters. Without explicit treatment of **Orchestration Patterns**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Orchestration Patterns: Supervisor, Parallel, Subgraph rests on [299, 2026], [306, 2026], and [312, 2026]. The lead source's own note reads: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for fixing what **Orchestration Patterns: Supervisor, Parallel, Subgraph** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Orchestration Patterns**, work from the cited evidence behind this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Orchestration Patterns**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Orchestration Patterns**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Orchestration Patterns** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Orchestration Patterns**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Orchestration Patterns** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

47.2.2.21 Lesson 21: Model Context Protocol (MCP): The USB Standard for Agentic AI Concept. Model Context Protocol (MCP): The USB Standard for Agentic AI evaluates tool protocols by allowlists, logging, provenance of retrieved content, and deny-by-default policies.

Why it matters. Analysts use **Model Context Protocol (MCP)** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that treating pattern names as deployment playbooks would otherwise hide, and the reviewer accountable for challenge.

Source support. Model Context Protocol (MCP): The USB Standard for Agentic AI rests on [155, 2026], [156, 2026], and [157, 2026]. The closest source to this row notes: The article explains how MCP acts as middleware between models and downstream services and surveys associated security risks, including overly broad permissions, unvetted servers, exposed endpoints, and limited monitoring. Use them for the working definition that **Model Context Protocol (MCP): The USB Standard for Agentic AI** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Model Context Protocol (MCP)** in the evidence the row cites. [155, 2026] Radosevich and Halloran (2025) audit security vulnerabilities in Anthropic's Model Context Protocol (MCP), which allows LLMs to integrate with external tools and data sources. The authors demonstrate that language models using MCP can be manipulated through prompt injection to execute malicious code, enable remote access, and steal credentials. [156, 2026] A Protect AI blog post (April 2025) introducing the Model Context Protocol (MCP), the open-source layer Anthropic introduced in November 2024 to standardize how large language model applications connect to data sources and tools. The article explains how MCP acts as middleware between models and downstream services and surveys associated security risks, including overly broad permissions, unvetted servers, exposed endpoints, and limited monitoring. [157, 2026] This is a Bandwidth blog post explaining how the Model Context Protocol (MCP) supports agentic AI systems that can assess context and take actions rather than only respond to prompts. Using a contact-center voice agent example, it describes MCP as a standard for letting AI models interact securely with external tools, APIs, and data sources, and covers instructions versus multi-step workflows. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Model Context Protocol (MCP)**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Model Context Protocol**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Model Context Protocol (MCP)** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Model Context Protocol (MCP)**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Model Context Protocol (MCP)** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

47.2.2.22 Lesson 22: MCP Architecture: Client, Server, Host Concept. MCP Architecture: Client, Server, Host evaluates tool protocols by allowlists, logging, provenance of retrieved content, and deny-by-default policies.

Why it matters. MCP Architecture: Client, Server, Host matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; treating pattern names as deployment playbooks is a common failure.

Source support. MCP Architecture: Client, Server, Host rests on [299, 2026], [306, 2026], and [312, 2026]. Its anchor reference records: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for the claim that **MCP Architecture: Client, Server, Host** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **MCP Architecture: Client, Server, Host**, work from the cited evidence behind this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **MCP Architecture**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **MCP Architecture**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **MCP Architecture: Client, Server, Host** work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **MCP Architecture: Client, Server, Host**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **MCP Architecture: Client, Server, Host** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

47.2.2.23 Lesson 23: NSA Security Design Considerations for MCP

Concept. NSA Security Design Considerations for MCP studies the declassified record for institutional lessons about oversight, source protection, and limits on translating history into practice.

Why it matters. Analysts use **NSA Security Design Considerations** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that treating pattern names as deployment playbooks would otherwise hide, and the reviewer accountable for challenge.

Source support. NSA Security Design Considerations for MCP rests on [155, 2026]. The closest source to this row notes: Radosevich and Halloran (2025) audit security vulnerabilities in Anthropic's Model Context Protocol (MCP), which allows LLMs to integrate with external tools and data sources. Use it for pinning down the scope of **NSA Security Design Considerations for MCP**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **NSA Security Design Considerations**, work from the cited evidence behind this row. [155, 2026] Radosevich and Halloran (2025) audit security vulnerabilities in Anthropic's Model Context Protocol (MCP), which allows LLMs to integrate with external tools and data sources. The authors demonstrate that language models using MCP can be manipulated through prompt injection to execute malicious code, enable remote access, and steal credentials. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **NSA Security Design Considerations**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **NSA Security Design Considerations for**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **NSA Security Design Considerations** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **NSA Security Design Considerations**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **NSA Security Design Considerations** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

47.2.2.24 Lesson 24: MCP Security Risks: Tool Poisoning, Prompt Injection via Server

Concept. MCP Security Risks: Tool Poisoning, Prompt Injection via Server evaluates tool protocols by allowlists, logging, provenance of retrieved content, and deny-by-default policies.

Why it matters. MCP Security Risks matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; treating pattern names as deployment playbooks is a common failure.

Source support. MCP Security Risks: Tool Poisoning, Prompt Injection via Server rests on [159, 2026]. Its anchor reference records: It identifies concerns including weak default authentication, supply-chain exposure from compromised tools, over-permissioned access tokens, injection and context-poisoning attacks, and gaps in audit logging for agentic workflows. Use it for fixing what **MCP Security Risks: Tool Poisoning, Prompt Injection via Server** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **MCP Security Risks**, reason from the sources cited in this row. [159, 2026] A September 2025 Bitdefender Business Insights article by Martin Zugec examining security risks in the Model Context Protocol, the standard introduced by Anthropic for connecting AI agents to external tools and data. It identifies concerns including weak default authentication, supply-chain exposure from compromised tools, over-permissioned access tokens, injection and context-poisoning attacks, and gaps in audit logging for agentic workflows. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **MCP Security Risks**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **MCP Security Risks**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **MCP Security Risks** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **MCP Security Risks**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **MCP Security Risks** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

47.2.2.25 Lesson 25: MCP in Intelligence Workflows: Structured Tool Registration

Concept. MCP in Intelligence Workflows: Structured Tool Registration evaluates tool protocols by allowlists, logging, provenance of retrieved content, and deny-by-default policies.

Why it matters. MCP in Intelligence Workflows connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. MCP in Intelligence Workflows: Structured Tool Registration rests on [299, 2026], [306, 2026], and [312, 2026]. The most specific cited work observes: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM

applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for the claim that **MCP in Intelligence Workflows: Structured Tool Registration** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **MCP in Intelligence Workflows** against the works cited for this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **MCP in Intelligence Workflows**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **MCP in Intelligence Workflows**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **MCP in Intelligence Workflows** work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **MCP in Intelligence Workflows**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **MCP in Intelligence Workflows** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

47.2.2.26 Lesson 26: Agent-to-Agent (A2A) Protocols: Interoperability Between Frameworks

Concept. Agent-to-Agent (A2A) Protocols: Interoperability Between Frameworks treats agents as software actors with explicit permissions, logs, stop conditions, and human approval—not autonomous decision makers.

Why it matters. Without explicit treatment of **Agent-to-Agent (A2A) Protocols: Interoperability Between Frameworks**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Agent-to-Agent (A2A) Protocols: Interoperability Between Frameworks rests on [137, 2026]. The closest source to this row notes: An arXiv paper surveying the shift from passive language models to Agentic AI, where large language models act as cognitive controllers that combine memory, tool use, and environmental feedback to pursue extended goals. Use it for the working definition that **Agent-to-Agent (A2A) Protocols: Interoperability Between Frameworks** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Agent-to-Agent (A2A) Protocols: Interoperability Between Frameworks** in the evidence the row cites. [137, 2026] An arXiv paper surveying the shift from passive language models to Agentic AI, where large language models act as cognitive controllers that combine memory, tool use, and environmental feedback to pursue extended goals. It proposes a unified taxonomy organizing agent systems into six components: perception, brain, planning, action, tool use, and collaboration. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Agent-to-Agent (A2A) Protocols**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Agent-to-Agent Protocols**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **Agent-to-Agent (A2A) Protocols: Interoperability Between Frameworks** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Agent-to-Agent (A2A) Protocols: Interoperability Between Frameworks**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Agent-to-Agent (A2A) Protocols: Interoperability Between Frameworks** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

47.2.2.27 Lesson 27: n8n and Make.com: No-Code/Low-Code Agentic Intelligence Pipelines

Concept. n8n and Make.com: No-Code/Low-Code Agentic Intelligence Pipelines uses the pattern name as safe architectural vocabulary: allowlisted tools, logging, human approval, and blocked external action.

Why it matters. n8n and Make.com: No-Code/Low-Code Agentic Intelligence Pipelines connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. n8n and Make.com: No-Code/Low-Code Agentic Intelligence Pipelines rests on [153, 2026]. Its anchor reference records: The second half of the framework highlights common agentic frameworks. Use it for the working definition that **n8n and Make.com: No-Code/Low-Code Agentic Intelligence Pipelines** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **n8n and Make.com: No-Code/Low-Code Agentic Intelligence Pipelines** in the evidence the row cites. [153, 2026] The second half of the framework highlights common agentic frameworks. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **n8n and Make.com**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **n8n and Make com**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape **n8n and Make.com: No-Code/Low-Code Agentic Intelligence Pipelines** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **n8n and Make.com: No-Code/Low-Code Agentic Intelligence Pipelines**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **n8n and Make.com: No-Code/Low-Code Agentic Intelligence Pipelines** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

47.2.2.28 Lesson 28: Top 8 Agentic AI Frameworks Comparison (2026)

Concept. Top 8 Agentic AI Frameworks Comparison (2026) evaluates agentic-AI governance claims against OECD principles: transparency, accountability, and human oversight.

Why it matters. Without explicit treatment of **Top 8 Agentic AI Frameworks Comparison (2026)**, treating pattern names as deployment playbooks undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Top 8 Agentic AI Frameworks Comparison (2026) rests on [146, 2026]. The closest source to this row notes: An Exabeam explainer describing agentic AI frameworks as software toolkits that provide pre-built components and architectures for building autonomous AI agents. Use it for fixing what **Top 8 Agentic AI Frameworks Comparison (2026)** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Top 8 Agentic AI Frameworks Comparison (2026)**, work from the cited evidence behind this row. [146, 2026] An Exabeam explainer describing agentic AI frameworks as software toolkits that provide pre-built components and architectures for building autonomous AI agents. It outlines core elements such as agent coordination, tool integration, memory management, workflow definition, and deployment monitoring, and reviews eight frameworks including LangGraph, AutoGen, CrewAI, LlamaIndex, Haystack, DSPy, and Semantic Kernel. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Top 8 Agentic AI Frameworks Comparison (2026)**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the pattern descriptor, the bounded claim about **Top 8 Agentic AI Frameworks**, the safe-substitution caveat, the uncertainty note, the no-deployment boundary, and the reviewer accountable for challenge. Shape this subject work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Top 8 Agentic AI Frameworks Comparison (2026)**: that naming an agent pattern certifies it is safe to deploy without governance gates.

Transfer task. Transfer **Top 8 Agentic AI Frameworks Comparison (2026)** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

47.2.3 AGEINT Frameworks and Infrastructure worked safe example: synthetic inputs, evidence, and review

Worked example: a synthetic research assistant agent organizes public readings for an instructor. [255, 2026]; [256, 2026].

Triangulation anchors. In module 33's worked-example section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **governed agentic intelligence**. Learners use a **agent run and assurance card** and keep this boundary visible: No autonomous external action, credentialed operations, live-target workflows, or uncontrolled tool use.

Frame. The classroom question centers on **LangChain/LangGraph: State Machine Orchestration**. Excluded actions stay explicit, and the **Agentic Tool-Governance Lens** planning question is: Which human authority, agent identity, tool permission, autonomy limit, incident threshold, and recoverability condition bounds the workflow?

Inputs. For the **LangChain/LangGraph: State Machine Orchestration** scenario, use public URLs, a fixed retrieval tool, a summarization prompt, a time budget, and a stop condition. The Agentic Tool-Governance Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **LangChain/LangGraph: State Machine Orchestration**, students bind the agent identity, list allowed tools, set autonomy limits, capture sources, block unsafe requests, and log approvals. Pause whenever an inference about LangChain/LangGraph: State Machine Orchestration appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **LangChain/LangGraph: State Machine Orchestration** classroom scenario; unit artifact = agent run and assurance card; evidence = allowed inputs; method = least-privilege agent design and run review; output = an agent run card with tool calls, source links, blocked actions, reviewer notes, incident threshold, and recovery decision; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **LangChain/LangGraph: State Machine Orchestration** as "Agentic Tool-Governance Lens confirms it" is not enough. The revision ties the claim to least-privilege agent design and run review, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **LangChain/LangGraph: State Machine Orchestration** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

47.2.4 Agentic Tool-Governance Lens path for AGEINT Frameworks and Infrastructure: lesson cluster, safe artifact, and review (continued 2)

Evidence anchor. Section 47; [OECD, 2026a].

47.2.5 AGEINT Frameworks and Infrastructure practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Agentic Tool-Governance Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**. **Triangulation anchors.** In module 33's practice-sequence section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare LangChain/LangGraph: State Machine Orchestration, LCEL: LangChain Expression Language, LangGraph: Stateful, Cyclical Agentic Workflows; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Agentic AI Governance and Tool Security** lane.
2. Frame	Answer the lens question: Which human authority, agent identity, tool permission, autonomy limit, incident threshold, and recoverability condition bounds the workflow?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for LangChain/LangGraph: State Machine Orchestration: agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the agent run and assurance card fields for LangChain/LangGraph: State Machine Orchestration.	Unit profile note.	Evidence artifacts include tool-allowlist record, external-memory governance boundary.
4. Challenge	Test the misconception that naming an agent pattern certifies it is safe to deploy without governance gates.	Failure-mode note.	The artifact applies the key distinction: separate agent assistance from autonomous external action.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

47.2.5.1 AGEINT Frameworks and Infrastructure instructor notes: source reasoning, review points, and studio focus Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**. [255, 2026]; [256, 2026].

47.2.5.2 AGEINT Frameworks and Infrastructure extension exercise: peer validation and refresh trigger review **Evidence anchor.** Section 47; [255, 2026].

Have learners swap artifacts and apply the **Agentic Tool-Governance Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**.

47.2.6 AGEINT Frameworks and Infrastructure knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 47; [255, 2026].

1. Explain how **LangChain/LangGraph: State Machine Orchestration** is defined here; name the source descriptor that supports the definition.
2. Contrast **LangChain/LangGraph: State Machine Orchestration** with **LCEL: LangChain Expression Language** using the **Agentic Tool-Governance Lens** artifact fields.
3. Identify one failure mode from the **Agentic AI Governance and Tool Security** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which permission can be removed while preserving the learning objective?
5. Correct this misconception: that naming an agent pattern certifies it is safe to deploy without governance gates.

47.2.6.1 AGEINT Frameworks and Infrastructure answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **LangChain/LangGraph: State Machine Orchestration** without source evidence, uncertainty, or a safe transfer task.

47.3 AGEINT Frameworks and Infrastructure assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 47; [255, 2026].

47.3.1 AGEINT Frameworks and Infrastructure evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 47; [255, 2026].

47.3.2 AGEINT Frameworks and Infrastructure transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 47; [255, 2026].

47.3.2.1 AGEINT Frameworks and Infrastructure lineage and source tradition: profile, concepts, and first anchors This sits in the **Agentic AI Governance and Tool Security** lineage: delegated action under explicit authority, identity, permissions, tool boundaries, monitoring, and human escalation. [255, 2026]; [256, 2026].

47.3.2.2 AGEINT Frameworks and Infrastructure working model: inputs, constraints, transforms, outputs, and oversight Evidence anchor. Section 47; [255, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**, with provenance and reviewability throughout.

47.3.2.3 AGEINT Frameworks and Infrastructure knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [255, 2026]; [256, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

47.3.2.4 AGEINT Frameworks and Infrastructure transfer contracts: authority, evidence, tools, and auditable output Evidence anchor. Section 47; [255, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**.
- **Evidence contract:** keep the **Agentic AI Governance and Tool Security** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

47.3.2.5 AGEINT Frameworks and Infrastructure profile emphasis and local focus: method stack and topic cluster Evidence anchor. Section 47; [255, 2026].

The matched profile emphasizes delegated action under explicit authority, identity, permissions, tool boundaries, monitoring, and human escalation. The method stack is AI RMF Govern-Map-Measure-Manage, least-privilege tool design, prompt-injection review, progressive deployment, and rollback drills; the local topic cluster is **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**.

47.3.3 AGEINT Frameworks and Infrastructure evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 47; [255, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Agentic AI Governance and Tool Security** profile tells reviewers what evidence is strong enough for the module artifact built around **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**.

47.3.3.1 AGEINT Frameworks and Infrastructure guide source spine: inherited keys and local citation roles Primary guide citations: [255, 2026]; [256, 2026]; [258, 2026]; [273, 2026]; [274, 2026]; [275, 2026]; [286, 2026]; [287, 2026]; [292, 2026]; [147, 2026]; [153, 2026]; [154, 2026]; [144, 2026]; [155, 2026]; [156, 2026]; [157, 2026]; [158, 2026]; [159, 2026]; [137, 2026]; [146, 2026]; [299, 2026]; [306, 2026]; [312, 2026].

47.3.3.2 AGEINT Frameworks and Infrastructure verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [255, 2026]; [256, 2026].

Tier	What counts	How it is used
Source guide	[255, 2026]; [256, 2026]; [258, 2026]; [273, 2026]; [274, 2026]; [275, 2026]; [286, 2026]; [287, 2026]; [292, 2026]; [147, 2026]; [153, 2026]; [154, 2026]; [144, 2026]; [155, 2026]; [156, 2026]; [157, 2026]; [158, 2026]; [159, 2026]; [137, 2026]; [146, 2026]; [299, 2026]; [306, 2026]; [312, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 33's source-canon section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language** and [255, 2026]; [256, 2026], but only directly verified source URLs are encoded as citations.

47.3.3.3 AGEINT Frameworks and Infrastructure intelligence practice lens: evidence artifact and safety check Practice lens: **Agentic Tool-Governance Lens** for **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**. [255, 2026]; [256, 2026].

Planning question: Which human authority, agent identity, tool permission, autonomy limit, incident threshold, and recoverability condition bounds the workflow?

Evidence artifact: agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path.

Validation rule: verify least privilege, prompt-injection exposure, provenance, observability, stop conditions, and incident-reporting triggers. Applied to **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**.

Handoff contract: export agent traces, tool calls, retrieved sources, policy decisions, and human approvals separately.

Safety check: block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions.

47.3.3.4 AGEINT Frameworks and Infrastructure runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 47; [255, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	33.99	33.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind AGEINT Frameworks and Infrastructure to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
AGEINT pattern registry, agent identity, and interface-contract studio	33.100	33.100 source title transformed into safe curriculum treatment; original: V2 AGEINT-depth extension: map frameworks to interoperable tool descriptions, Web of Things affordances, OpenAPI contracts, credential semantics, revocation, and error-handling evidence	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Bounded autonomy, procurement, incident-response, and assurance studio	33.101	33.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for AGEINT Frameworks and Infrastructure	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Model-card, recoverability, retention, and learner-support evidence package	33.102	33.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for AGEINT Frameworks and Infrastructure	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
LangChain/LangGraph: State Machine Orchestration	33.1	33.1 LangChain/LangGraph: State Machine Orchestration	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
LCEL: LangChain Expression Language	33.1.1	33.1.1 LCEL: LangChain Expression Language	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
LangGraph: Stateful, Cyclical Agentic Workflows	33.1.2	33.1.2 LangGraph: Stateful, Cyclical Agentic Workflows	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
LangSmith: Observability and Tracing	33.1.3	33.1.3 LangSmith: Observability and Tracing	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
CrewAI: Role-Based Multi-Agent Collaboration	33.2	33.2 CrewAI: Role-Based Multi-Agent Collaboration	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Crew, Agent, Task, and Process Objects	33.2.1	33.2.1 Crew, Agent, Task, and Process Objects	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Sequential, Parallel, and Hierarchical Process Modes	33.2.2	33.2.2 Sequential, Parallel, and Hierarchical Process Modes	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Built-in Tool Ecosystem	33.2.3	33.2.3 Built-in Tool Ecosystem	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
AutoGen (Microsoft): Multi-Agent Conversation Patterns	33.3	33.3 AutoGen (Microsoft): Multi-Agent Conversation Patterns	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
AssistantAgent and UserProxyAgent Pattern	33.3.1	33.3.1 AssistantAgent and UserProxyAgent Pattern	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
GroupChat with RoundRobin and AutoSelect Managers	33.3.2	33.3.2 GroupChat with RoundRobin and AutoSelect Managers	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Agentic cyber-misuse control review using sample prompt records, fabricated logs, and deny-by-default tool policies	33.3.3	33.3.3 source title transformed into safe curriculum treatment; original: Code Execution Risk and Sandboxing Requirements	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Semantic Kernel: Enterprise AI Orchestration	33.4	33.4 Semantic Kernel: Enterprise AI Orchestration	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
AWS Agentic Patterns: Production Architecture Guide	33.5	33.5 AWS Agentic Patterns: Production Architecture Guide	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Basic Reasoning Agents	33.5.1	33.5.1 Basic Reasoning Agents	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Tool-Based Agents (Function Calling and MCP Servers)	33.5.2	33.5.2 Tool-Based Agents (Function Calling and MCP Servers)	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Computer-Use Agents	33.5.3	33.5.3 Computer-Use Agents	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Coding Agents	33.5.4	33.5.4 Coding Agents	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Speech-to-Speech Agents	33.5.5	33.5.5 Speech-to-Speech Agents	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Orchestration Patterns: Supervisor, Parallel, Subgraph	33.5.6	33.5.6 Orchestration Patterns: Supervisor, Parallel, Subgraph	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Model Context Protocol (MCP): The USB Standard for Agentic AI	33.6	33.6 Model Context Protocol (MCP): The USB Standard for Agentic AI	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
MCP Architecture: Client, Server, Host	33.6.1	33.6.1 MCP Architecture: Client, Server, Host	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
NSA Security Design Considerations for MCP	33.6.2	33.6.2 NSA Security Design Considerations for MCP	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
MCP Security Risks: Tool Poisoning, Prompt Injection via Server	33.6.3	33.6.3 MCP Security Risks: Tool Poisoning, Prompt Injection via Server	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
MCP in Intelligence Workflows: Structured Tool Registration	33.6.4	33.6.4 MCP in Intelligence Workflows: Structured Tool Registration	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Agent-to-Agent (A2A) Protocols: Interoperability Between Frameworks	33.7	33.7 Agent-to-Agent (A2A) Protocols: Interoperability Between Frameworks	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
n8n and Make.com: No-Code/Low-Code Agentic Intelligence Pipelines	33.8	33.8 n8n and Make.com: No-Code/Low-Code Agentic Intelligence Pipelines	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Top 8 Agentic AI Frameworks Comparison (2026)	33.9	33.9 Top 8 Agentic AI Frameworks Comparison (2026)	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

47.3.3.5 AGEINT Frameworks and Infrastructure reusable subsection contract: topic rows, artifacts, and safety duties Evidence anchor. Section 47; [255, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
LangChain/LangGraph: State Machine Orchestration	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
LCEL: LangChain Expression Language	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
LangGraph: Stateful, Cyclical Agentic Workflows	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
LangSmith: Observability and Tracing	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
CrewAI: Role-Based Multi-Agent Collaboration	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Crew, Agent, Task, and Process Objects	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Sequential, Parallel, and Hierarchical Process Modes	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Built-in Tool Ecosystem	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
AutoGen (Microsoft): Multi-Agent Conversation Patterns	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
AssistantAgent and UserProxyAgent Pattern	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
GroupChat with RoundRobin and AutoSelect Managers	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

Lesson topic	Practice lens	Evidence artifact	Safety check
Agentic cyber-misuse control review using sample prompt records, fabricated logs, and deny-by-default tool policies	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Semantic Kernel: Enterprise AI Orchestration	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
AWS Agentic Patterns: Production Architecture Guide	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Basic Reasoning Agents	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Tool-Based Agents (Function Calling and MCP Servers)	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Computer-Use Agents	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Coding Agents	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Speech-to-Speech Agents	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Orchestration Patterns: Supervisor, Parallel, Subgraph	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Model Context Protocol (MCP): The USB Standard for Agentic AI	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
MCP Architecture: Client, Server, Host	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
NSA Security Design Considerations for MCP	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
MCP Security Risks: Tool Poisoning, Prompt Injection via Server	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
MCP in Intelligence Workflows: Structured Tool Registration	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Agent-to-Agent (A2A) Protocols: Interoperability Between Frameworks	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
n8n and Make.com: No-Code/Low-Code Agentic Intelligence Pipelines	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Top 8 Agentic AI Frameworks Comparison (2026)	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

47.3.3.6 AGEINT Frameworks and Infrastructure annotated source ledger: real titles and local contribution Each source cited by this **Agentic AI Governance and Tool Security** module is paired below with its real title and a one-line note on what it contributes to **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**.

Source	Cited work	What it contributes	Status
[255, 2026]	Web of Things (WoT) Architecture 1.1	The W3C Recommendation for Web of Things Architecture 1.1, published in December 2023, defining an abstract architecture for interoperability across diverse Internet of Things platforms. It introduces core concepts including Things described by machine-readable Thing Descriptions, reusable Thing Models, and Consumers that interpret descriptions to interact via Properties, Actions, and Events.	verified source-guide
[256, 2026]	Web of Things (WoT) Thing Description 1.1	The W3C WoT Thing Description 1.1 is a formal information model and standardized representation format enabling IoT devices to describe their metadata and interaction capabilities in a machine-readable way, facilitating interoperability across diverse ecosystems.	verified source-guide
[258, 2026]	OpenAPI Specification	The official OpenAPI Initiative publications page, serving as a central index for the OpenAPI Specification and related standards including the Arazzo and Overlay specifications. It provides access to multiple specification versions (2.0, 3.0, 3.1, and 3.2) and their corresponding downloadable schemas identified by release date, along with a registry of extensions, formats, media types, and other resources.	verified source-guide
[273, 2026]	WCAG 2 Overview	The W3C Web Accessibility Initiative overview of the Web Content Accessibility Guidelines (WCAG), an international standard for making web content accessible to people with disabilities. It explains that WCAG is organized around four principles (perceivable, operable, understandable, robust) with testable success criteria at three conformance levels (A, AA, AAA), and covers versions 2.0, 2.1, and 2.2.	verified source-guide
[274, 2026]	CAST Universal Design for Learning Guidelines version 3.0	The official CAST website for the Universal Design for Learning (UDL) Guidelines version 3.0, released in 2024. The framework offers research-based guidance for designing inclusive learning environments and is organized around three principles: Engagement (motivation and emotional support), Representation (accessible presentation of information), and Action and Expression (diverse means of participation and communication).	verified source-guide
[275, 2026]	Fact Sheet: New Rule on the Accessibility of Web Content and Mobile Apps Provided by State and Local Governments	A US Department of Justice fact sheet explaining the 2024 ADA Title II rule requiring state and local governments to make their web content and mobile apps accessible. It establishes WCAG 2.1 Level AA as the technical standard, applies to entities such as schools, courts, libraries, and transit agencies, and sets compliance deadlines of April 2027 for larger jurisdictions and April 2028 for smaller ones.	verified source-guide

Source	Cited work	What it contributes	Status
[286, 2026]	Model Cards for Model Reporting	The arXiv abstract for "Model Cards for Model Reporting" (2018) by Mitchell, Wu, Zaldivar, and colleagues, which introduces a framework for transparent documentation of machine learning models. Model cards are short accompanying documents that report a model's benchmarked performance across varied conditions, including different cultural, demographic, and phenotypic groups, along with intended use, evaluation methodology, and deployment considerations.	verified source-guide
[287, 2026]	Datasheets for Datasets	A 2018 arXiv paper proposing 'datasheets for datasets,' a standardized documentation framework for machine learning datasets modeled on electronic component datasheets. The authors argue the field lacks consistent dataset documentation, which creates risk in high-stakes applications, and propose that datasets be accompanied by documentation covering motivation, composition, collection process, recommended uses, and test results.	verified source-guide
[292, 2026]	Assessing Risks and Impacts of AI (ARIA): Pilot Evaluation Report	The ARIA 0.1 pilot evaluation report documents NIST's methodology for systematically assessing AI applications for risks and societal impacts, using a multi-layered evaluation approach across five participating organizations and seven submitted AI applications. The pilot employed three evaluation scenarios and three testing levels: model testing, red teaming, and field testing, supplemented by dialogue annotation, tester questionnaires, and structured measurement trees.	verified source-guide
[147, 2026]	Agent Framework Security	Security analysis of major AI agent frameworks including LangChain, CrewAI, AutoGen, Semantic.	original practitioner context; secondary evidence only
[153, 2026]	Agentic AI is exploding, but which framework should you bet on?	The second half of the framework highlights common agentic frameworks.	original practitioner context; secondary evidence only
[154, 2026]	CrewAI	The homepage of CrewAI, a commercial platform for building, deploying, and managing AI agents at scale for enterprises. It presents the product as covering the full lifecycle from identifying automation opportunities to launching and optimizing multi-agent workflows while maintaining enterprise-level control.	verified source-guide
[144, 2026]	Agentic AI patterns and workflows on AWS	An AWS Prescriptive Guidance document (July 2025) introducing agentic AI patterns and workflows. It presents reusable design templates for building AI agent systems that operate with autonomy while remaining controllable and aligned with goals, aimed at architects, developers, and product leaders.	verified practitioner context; secondary evidence only

Source	Cited work	What it contributes	Status
[155, 2026]	Model Context Protocol (MCP): Security Design Considerations	Radosevich and Halloran (2025) audit security vulnerabilities in Anthropic's Model Context Protocol (MCP), which allows LLMs to integrate with external tools and data sources. The authors demonstrate that language models using MCP can be manipulated through prompt injection to execute malicious code, enable remote access, and steal credentials.	verified source-guide
[156, 2026]	MCP Security 101: A New Protocol for Agentic AI - Protect AI	A Protect AI blog post (April 2025) introducing the Model Context Protocol (MCP), the open-source layer Anthropic introduced in November 2024 to standardize how large language model applications connect to data sources and tools. The article explains how MCP acts as middleware between models and downstream services and surveys associated security risks, including overly broad permissions, unvetted servers, exposed endpoints, and limited monitoring.	verified practitioner context; secondary evidence only
[157, 2026]	Building Agentic AI with MCP - Bandwidth	This is a Bandwidth blog post explaining how the Model Context Protocol (MCP) supports agentic AI systems that can assess context and take actions rather than only respond to prompts. Using a contact-center voice agent example, it describes MCP as a standard for letting AI models interact securely with external tools, APIs, and data sources, and covers instructions versus multi-step workflows.	verified practitioner context; secondary evidence only
[158, 2026]	AI Spotlight: MCP (Model Context Protocol) and Agentic AI systems	A Gravitee blog post explaining the Model Context Protocol (MCP), an open standard developed by Anthropic for how applications provide context and tools to large language models. It compares MCP to a universal connector that replaces custom per-tool integrations, describing an architecture of hosts, clients, and servers and benefits such as reusability, provider flexibility, and improved access controls. The post situates MCP within the broader growth of agentic AI systems.	verified practitioner context; secondary evidence only
[159, 2026]	Security Risks of Agentic AI: A Model Context Protocol (MCP	A September 2025 Bitdefender Business Insights article by Martin Zugec examining security risks in the Model Context Protocol, the standard introduced by Anthropic for connecting AI agents to external tools and data. It identifies concerns including weak default authentication, supply-chain exposure from compromised tools, over-permissioned access tokens, injection and context-poisoning attacks, and gaps in audit logging for agentic workflows.	verified practitioner context; secondary evidence only

Source	Cited work	What it contributes	Status
[137, 2026]	[2601.12560] Agentic Artificial Intelligence (AI)	An arXiv paper surveying the shift from passive language models to Agentic AI, where large language models act as cognitive controllers that combine memory, tool use, and environmental feedback to pursue extended goals. It proposes a unified taxonomy organizing agent systems into six components: perception, brain, planning, action, tool use, and collaboration.	verified source-guide
[146, 2026]	Agentic AI Frameworks: Key Components & Top 8 Options in 2026	An Exabeam explainer describing agentic AI frameworks as software toolkits that provide pre-built components and architectures for building autonomous AI agents. It outlines core elements such as agent coordination, tool integration, memory management, workflow definition, and deployment monitoring, and reviews eight frameworks including LangGraph, AutoGen, CrewAI, LlamaIndex, Haystack, DSPy, and Semantic Kernel.	verified source-guide
[299, 2026]	Model Context Protocol Specification	The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation).	verified source-guide context; use pinned MCP anchor for normative claims
[306, 2026]	Artificial Intelligence	Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support.	original source-guide
[312, 2026]	Guide on the Use of Agentic Artificial Intelligence	Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support.	original source-guide

Where this sits. This module's overview is Section 47; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

47.3.4 AGEINT Frameworks and Infrastructure governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 47; [255, 2026].

47.3.5 AGEINT Frameworks and Infrastructure analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 33's governance-boundary section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **Agentic AI Governance and Tool Security** for **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**. [255, 2026]; [256, 2026].

Curriculum topic spine: LangChain/LangGraph: State Machine Orchestration, **LCEL: LangChain Expression Language**, **LangGraph: Stateful, Cyclical Agentic Workflows**. **Verified anchor cluster:** [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]; [Community, 2020b]; [Community, 2020a]; [of the Director of National Intelligence, 2025b].

Conceptual depth: delegated action under explicit authority, identity, permissions, tool boundaries, monitoring, and human escalation.

Method stack: AI RMF Govern-Map-Measure-Manage, least-privilege tool design, prompt-injection review, progressive deployment, and rollback drills.

Composability contract: agents, tools, credentials, memory, retrieval stores, policies, and logs remain separately inspectable and revocable components.

Known failure modes: excessive agency, shadow tools, indirect prompt injection, memory poisoning, confused authority, and unbounded action chains.

Defensive boundary: agentic workflows stay synthetic, owned-lab, supervised, logged, rate-limited, and reversible unless a lawful production authority exists. Applied to **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**.

Anchor	Why it matters here
[OECD, 2026a]	Official OECD conceptual foundation for agentic AI. Checked as of 2026-05-21; role: source_quality_anchor.
[of Canada Secretariat, 2026a]	Government of Canada guide for accountable public-sector use of agentic AI, including governance, risk, transparency, testing, monitoring, and human oversight considerations. Checked as of 2026-05-24; role: curriculum_anchor.
[of Standards and Technology, 2023]	Official NIST.AI.100-1 risk-management framework. Checked as of 2026-05-21; role: source_quality_anchor.
[of Standards and Technology, 2024d]	Official NIST AI 600-1 generative AI profile. Checked as of 2026-05-21; role: source_quality_anchor.
[Community, 2020b]	Official IC principles for lawful, accountable, objective, human-centered, secure, resilient, and science-informed AI. Checked as of 2026-05-21; role: curriculum_anchor.
[Community, 2020a]	Official IC framework for AI goals, authorities, human judgment, bias mitigation, testing, documentation, explainability, and review. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2025b]	Official IC AI governance directive covering CAIO roles, oversight, interoperability, civil-liberties review, training data, and impact assessment. Checked as of 2026-05-21; role: curriculum_anchor.

47.3.5.1 AGEINT Frameworks and Infrastructure evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **Agentic AI Governance and Tool Security** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [255, 2026]; [256, 2026].

47.3.6 AGEINT Frameworks and Infrastructure agentic boundary: assist, approve, block, and record

Evidence anchor. Section 47; [255, 2026].

AGEINT translation is bounded by the **Agentic AI Governance and Tool Security** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**.

47.3.6.1 AGEINT Frameworks and Infrastructure permitted defensive utility: curriculum uses and safe outputs

Evidence anchor. Section 47; [255, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**.

47.3.6.2 AGEINT Frameworks and Infrastructure excluded operational boundary: blocked actions and stop rules

Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [255, 2026]; [256, 2026] and **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

47.3.7 AGEINT Frameworks and Infrastructure governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 47; [255, 2026].

Governance is practiced as a gate on the **Agentic AI Governance and Tool Security** lane. Learners use the **Agentic Tool-Governance Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**.

47.3.7.1 AGEINT Frameworks and Infrastructure governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [255, 2026]; [256, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Agentic AI Governance and Tool Security** failure modes and the **Agentic Tool-Governance Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

47.3.7.2 AGEINT Frameworks and Infrastructure evidence package handoff: appendices, records, and reuse **Evidence anchor.** Section 47; [255, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Agentic Tool-Governance Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**.

47.3.7.3 AGEINT Frameworks and Infrastructure current-source assurance: verified anchors and local artifact fit The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**. [255, 2026]; [256, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_oecd_agentic_ai` for **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**?	The Agentic AI Landscape and Its Conceptual Foundations; lane `source_quality_spine`; checked 2026-05-21.	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path; Official OECD conceptual foundation for agentic AI.
What does the module inherit from `official_canada_agentic_ai_guide` for **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**?	Guide on the Use of Agentic Artificial Intelligence; lane `public_sector_agentic_ai`; checked 2026-05-24.	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path; bounded-autonomy run card, recoverability review, approval threshold, monitoring evidence, and public-sector service assurance
What does the module inherit from `official_nist_ai_rmf` for **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**?	Artificial Intelligence Risk Management Framework (AI RMF 1.0); lane `source_quality_spine`; checked 2026-05-21.	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path; Official NIST.AI.100-1 risk-management framework.
What does the module inherit from `official_nist_ai_600_1` for **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**?	Artificial Intelligence Risk Management Framework: Generative AI Profile; lane `source_quality_spine`; checked 2026-05-21.	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path; Official NIST AI 600-1 generative AI profile.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 47; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

47.3.8 AGEINT Frameworks and Infrastructure assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 47; [255, 2026].

47.3.9 AGEINT Frameworks and Infrastructure assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 47; [255, 2026].

47.3.9.1 AGEINT Frameworks and Infrastructure capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**.
Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language** and [255, 2026]; [256, 2026].

47.3.9.2 AGEINT Frameworks and Infrastructure instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language** and [255, 2026]; [256, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

47.3.9.3 AGEINT Frameworks and Infrastructure assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
LangChain/LangGraph: State Machine Orchestration	Completed **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
LCEL: LangChain Expression Language	Completed **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
LangGraph: Stateful, Cyclical Agentic Workflows	Completed **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

47.3.10 AGEINT Frameworks and Infrastructure refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [255, 2026]; [256, 2026] and **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**.

47.3.10.1 AGEINT Frameworks and Infrastructure refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**. The local signals begin with [255, 2026]; [256, 2026].

47.3.10.2 AGEINT Frameworks and Infrastructure claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**, and the source spine for these checks begins with [255, 2026]; [256, 2026].

47.3.11 AGEINT Frameworks and Infrastructure reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [255, 2026]; [256, 2026].
Triangulation anchors. In module 33's review-checklist section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language**. [255, 2026]; [256, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

47.3.12 AGEINT Frameworks and Infrastructure learning-path links: module map, overview, and curriculum atlas

Use the cross-links below to place **LangChain/LangGraph: State Machine Orchestration; LCEL: LangChain Expression Language** in the wider unit: the orientation sets the frame, the parent unit supplies the shared safety posture, and the neighbouring modules show what evidence enters and leaves. Lead sources: [255, 2026]; [256, 2026].

Section 2, Section 44, Section 46, Section 48

48 AGEINT Security and Adversarial Considerations

48.0.1 AGEINT Security and Adversarial Considerations figures and course links: visual evidence, source flow, and navigation

The module uses Figure 92, Figure 93, Figure 94, Figure 95, Figure 96, Figure 97, Figure 98, Figure 99, Figure 100, Figure 101, Figure 102, Figure 103, and Figure 85 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.

Navigation links: Section 2, Section 44, Section 47, Section 49.

This module teaches the **Agentic AI Governance and Tool Security** lane through a bounded, source-backed coursebook chapter. [234, 2026]; [235, 2026].

48.1 Agentic AI Governance and Tool Security frame for AGEINT Security and Adversarial Considerations: source context, topic focus, and reader task

Evidence anchor. Section 48; [234, 2026].

48.1.1 AGEINT Security and Adversarial Considerations orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 48; [234, 2026].

48.1.2 AGEINT Security and Adversarial Considerations conceptual primer: source context, core model, and reader task

This chapter teaches agentic AI as delegated action under control: identity, authority, tool permissions, memory, logs, stop conditions, and recoverability define what an agent may do. The chapter uses **Defensive Cyber-Intelligence Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**.

The central distinction is to separate agent assistance from autonomous external action. Core topics include **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate; Cyber credential-and-movement taxonomy review using fabricated alerts**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.

Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [234, 2026]; [235, 2026].

Learners move from vocabulary and the **Defensive Cyber-Intelligence Lens** distinction through topic lessons on **Agent Framework Security Vulnerabilities** with evidence and misconception checks, then assemble a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** with safety and rights gates.

48.1.3 AGEINT Security and Adversarial Considerations learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 48; [234, 2026].

- Connect **Agent Framework Security Vulnerabilities and Python REPL sandbox and approval-gate** to **Agentic AI Governance and Tool Security** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate agent assistance from autonomous external action; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as excessive agency, shadow tools, indirect prompt injection, memory poisoning, confused authority, and unbounded action chains, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: agentic workflows stay synthetic, owned-lab, supervised, logged, rate-limited, and reversible unless a lawful production authority exists.

48.1.4 AGEINT Security and Adversarial Considerations core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 48; [234, 2026].

Term	Working definition
Agent identity	the named software actor, role, and authorization context for a run
Tool allowlist	the bounded set of actions the agent may request
Delegation	the handoff of a task under explicit human authority and review
Bounded autonomy	the documented ceiling on what an agent may decide or request without review
Recoverability	the path back to a known-safe state after a bad output or action request
AI incident	a logged event where an AI system creates or plausibly creates harm or loss of control
Prompt injection	untrusted content that attempts to override instructions or authority boundaries
Pattern registry	the catalog of approved agent behaviors, prompts, and evaluation hooks
Adversarial eval	structured tests that probe agent misuse, injection, and over-delegation before release
Agent Framework Security Vulnerabilities	Key terms: Agent, Framework, Security.
Python REPL sandbox and approval-gate	Key terms: Python, REPL, sandbox.

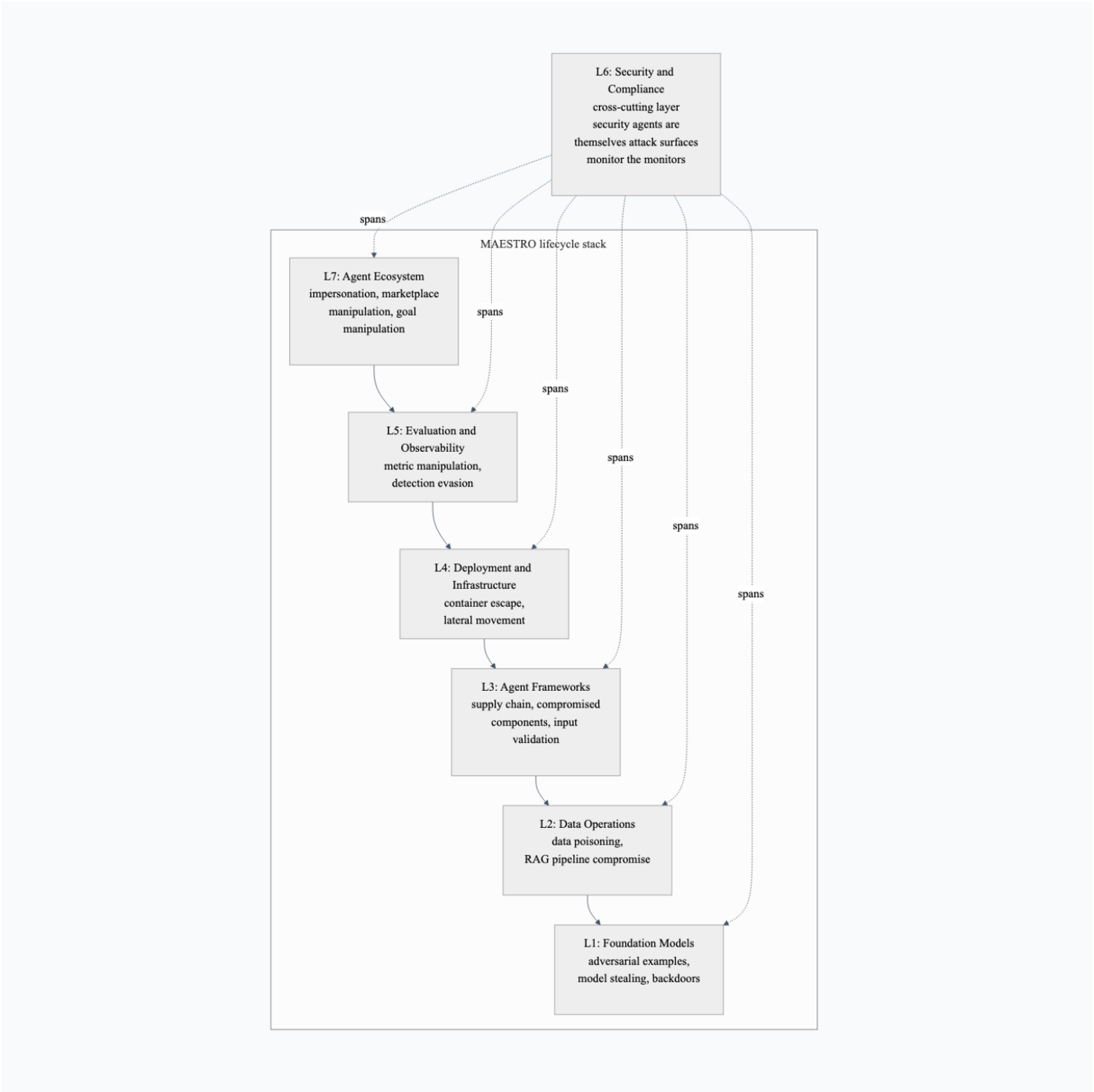


Figure 92: The CSA MAESTRO model stacks seven layers of the agentic AI lifecycle, with the L6 Security/Compliance layer cross-cutting every other layer because security agents are themselves attack surfaces. It is anchored to the ageint agentic intelligence / ageint security and adversarial considerations section; use it to inspect L6: Security and Compliance cross-cutting layer security agents are themselves attack surfaces monitor the monitors, MAESTRO lifecycle stack, L7: Agent Ecosystem impersonation, marketplace manipulation, goal manipulation, and L5: Evaluation and Observability metric manipulation, detection evasion while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

Figure 93: The author-defined SRE circuit-breaker teaching pattern state diagram shows when a supervised agent remains CLOSED, when safety-budget exhaustion forces OPEN human takeover, and how HALF_OPEN restoration is constrained by validation evidence. It is anchored to the ageint agentic intelligence / ageint security and adversarial considerations section; use it to inspect CLOSED normal supervised operation, OPEN human takeover after policy, provider, timeout, trust, or reasoning-loop triggers, HALF_OPEN limited restoration after recovery validation, and clean-record return path while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

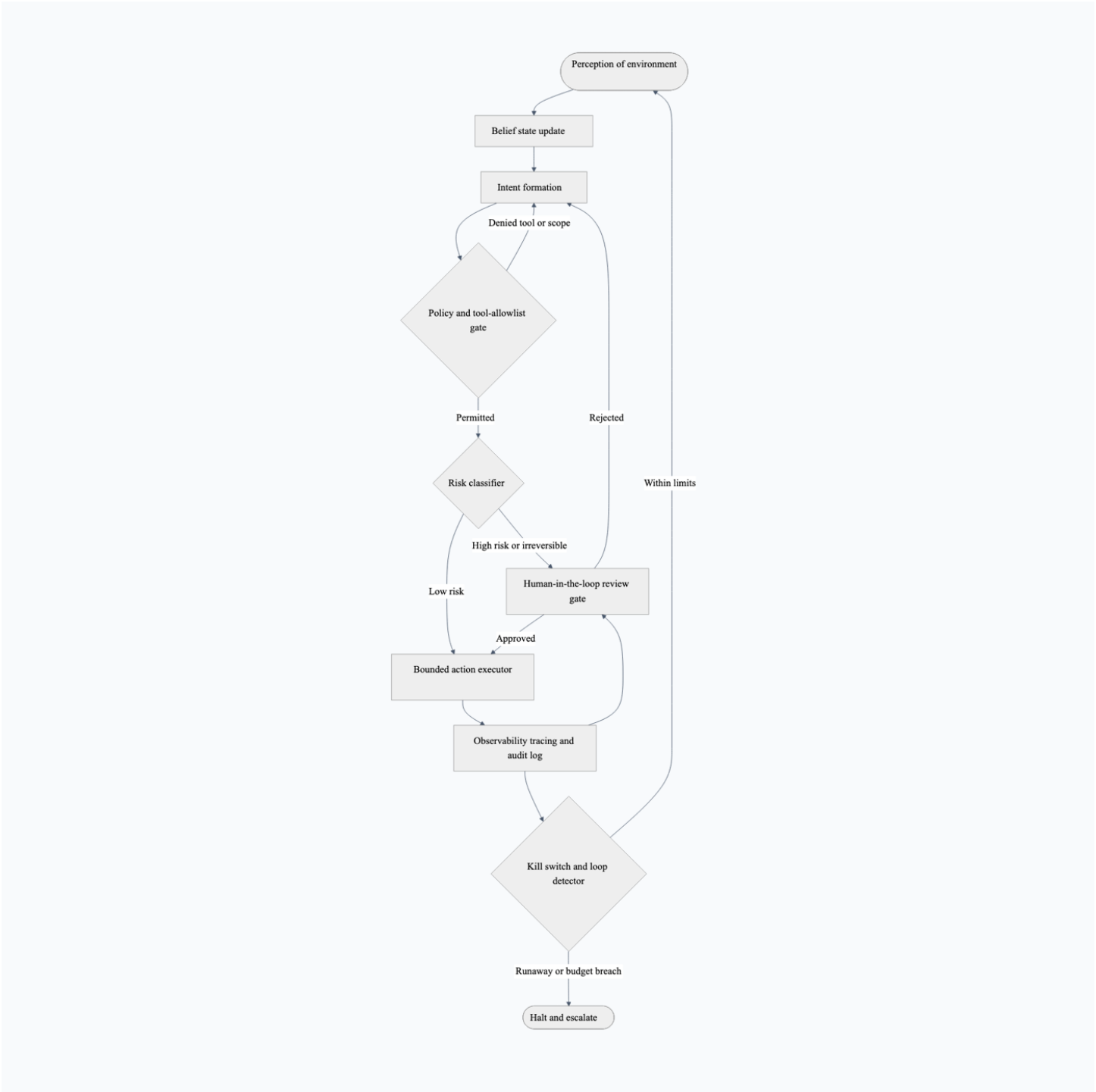


Figure 94: This diagram shows how an agentic intelligence system is bounded by least-privilege tooling, human review gates, observability, and kill-switch stop conditions before any action takes effect. It is anchored to the ageint agentic intelligence / ageint security and adversarial considerations section; use it to inspect A top-to-bottom governance . Perception feeds belief update, which feeds intent formation. Intent passes through a policy, tool-allowlist gate. A risk classifier branches to either a human-in-the- review gate for high-risk actions or a bounded action executor for low-risk actions. The human gate also reaches the executor. The executor sends results to an observability log, and which feeds both a kill-switch detector while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

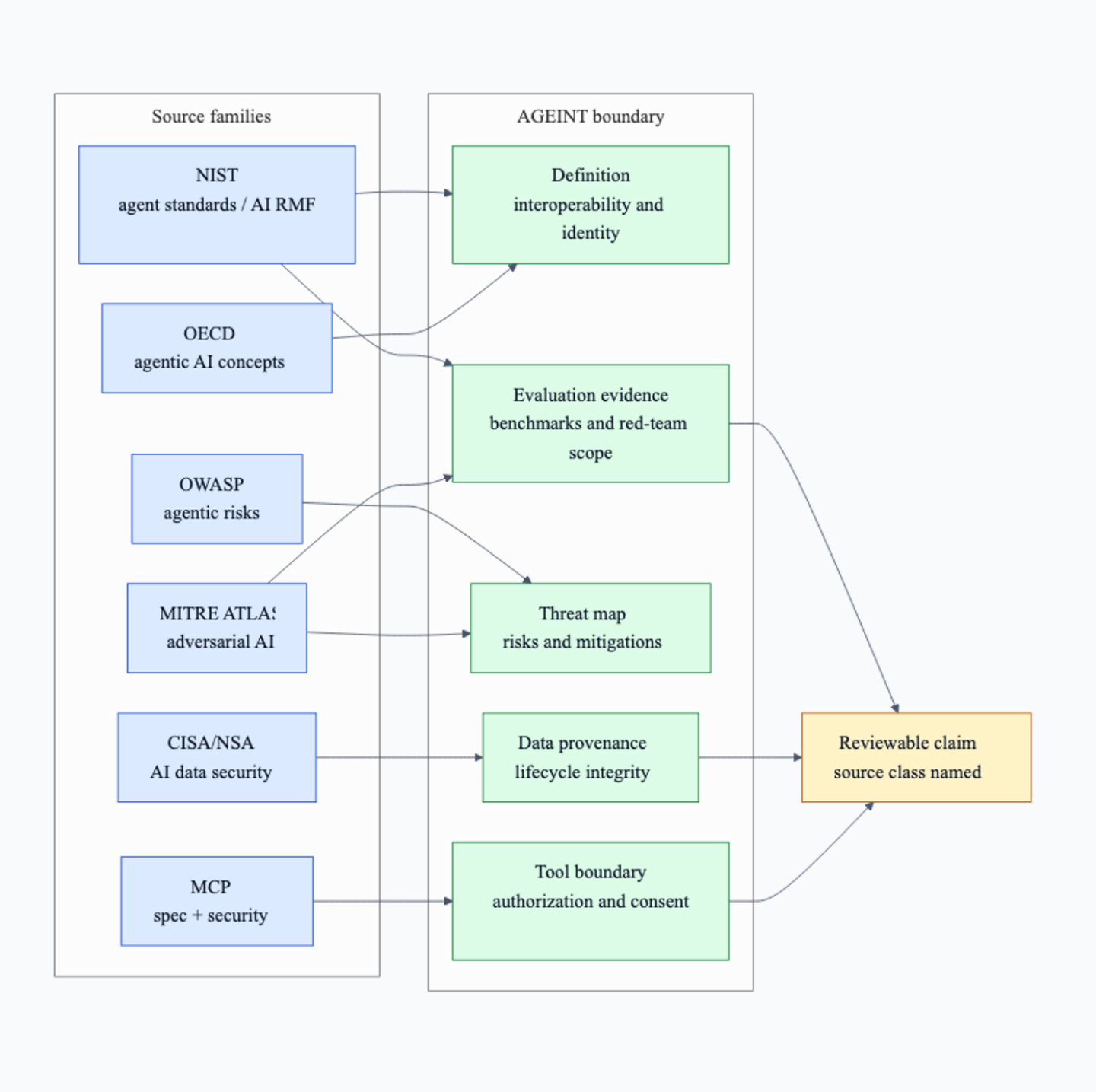


Figure 95: Source-backed conceptual schematic crosswalking current official and standards sources for agent identity, protocol boundaries, security threats, data provenance, and adversarial assurance. In the ageint agentic intelligence / ageint security and adversarial considerations section, it lets readers compare Source families, NIST agent standards / AI RMF, OECD agentic AI concepts, and MCP spec + security so the visual functions as a traceable course aid rather than an unscoped assertion.

Figure 96: The agent-evaluation sequence shows how benchmark purpose, context, automated runs, TEVV or red-team challenge, report caveats, and reviewer decisions must stay separate before AGEINT allows a bounded claim. Its reader value is to make evaluation purpose owner, benchmark context, automated benchmark evidence, TEVV or red-team challenge, report caveats, reviewer decision, bounded claim release, revise-and-retest loop for insufficient evidence visible at a glance, with the ageint agentic intelligence / ageint security and adversarial considerations section as the source section and defensive review as the boundary.

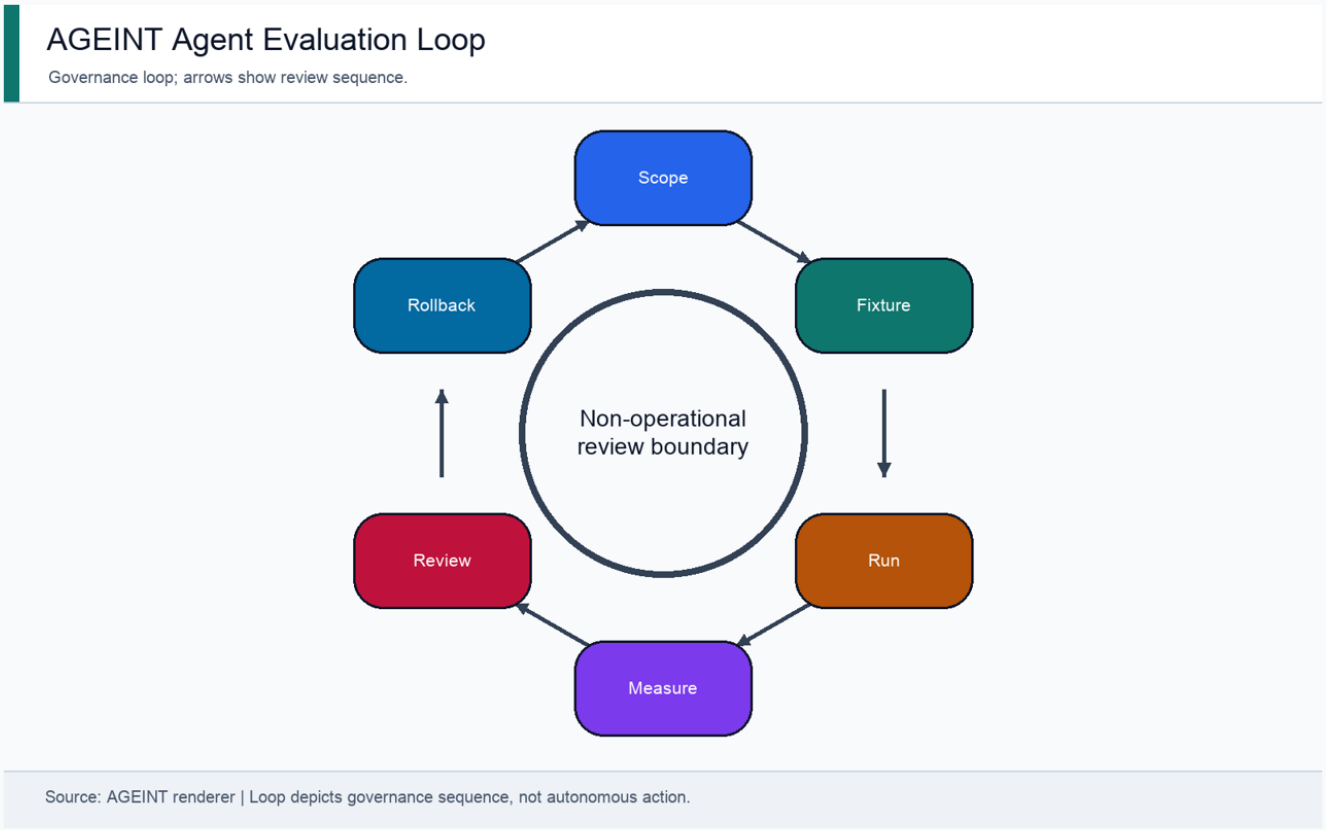


Figure 97: The agent evaluation loop places assurance, human review, and rollback before reuse. It is anchored to the ageint agentic intelligence / ageint security and adversarial considerations section; use it to inspect agent evaluation loop steps, decision gates, owner handoffs, refresh triggers, and closure evidence while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

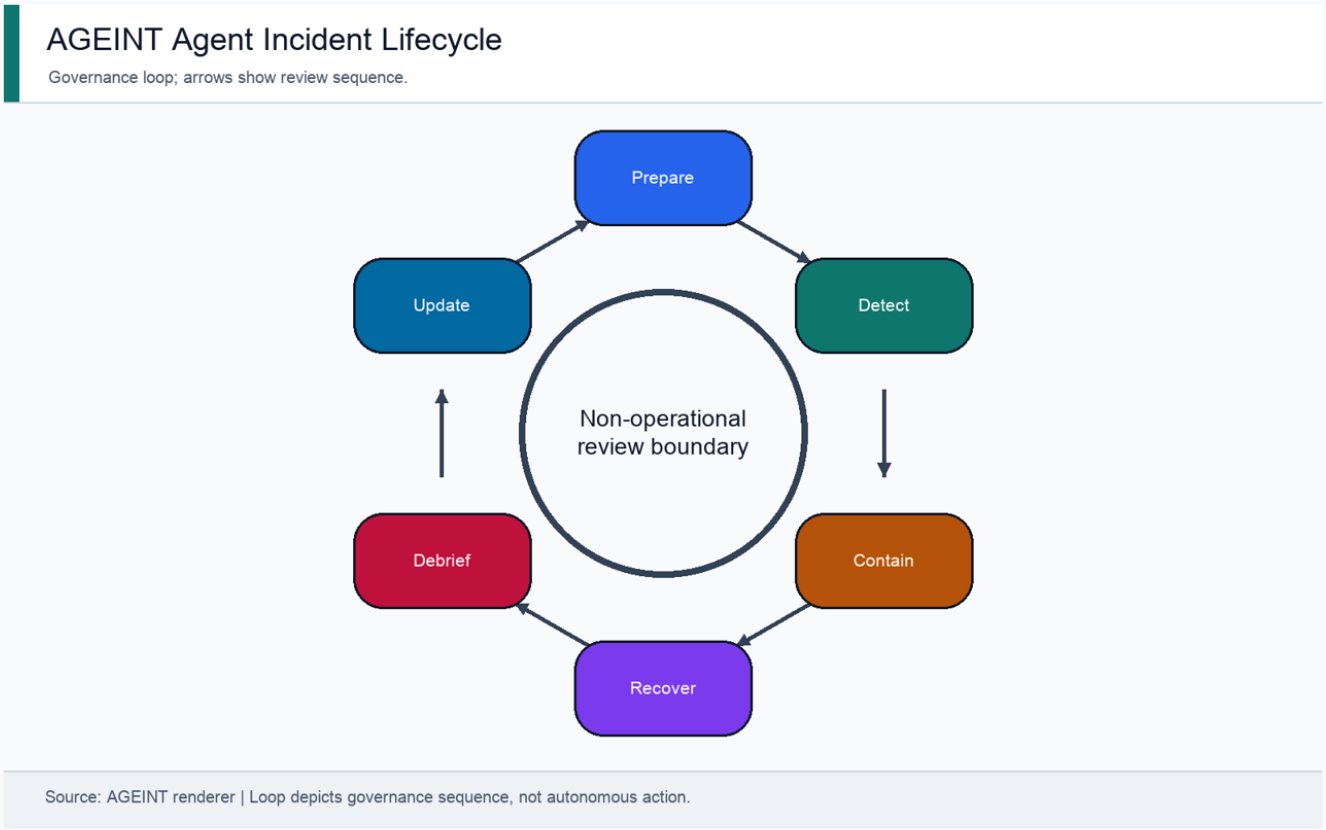


Figure 98: The agent incident lifecycle organizes preparation, detection, containment, recovery, and debrief learning. It is anchored to the ageint agentic intelligence / ageint security and adversarial considerations section; use it to inspect agent incident lifecycle steps, decision gates, owner handoffs, refresh triggers, and closure evidence while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

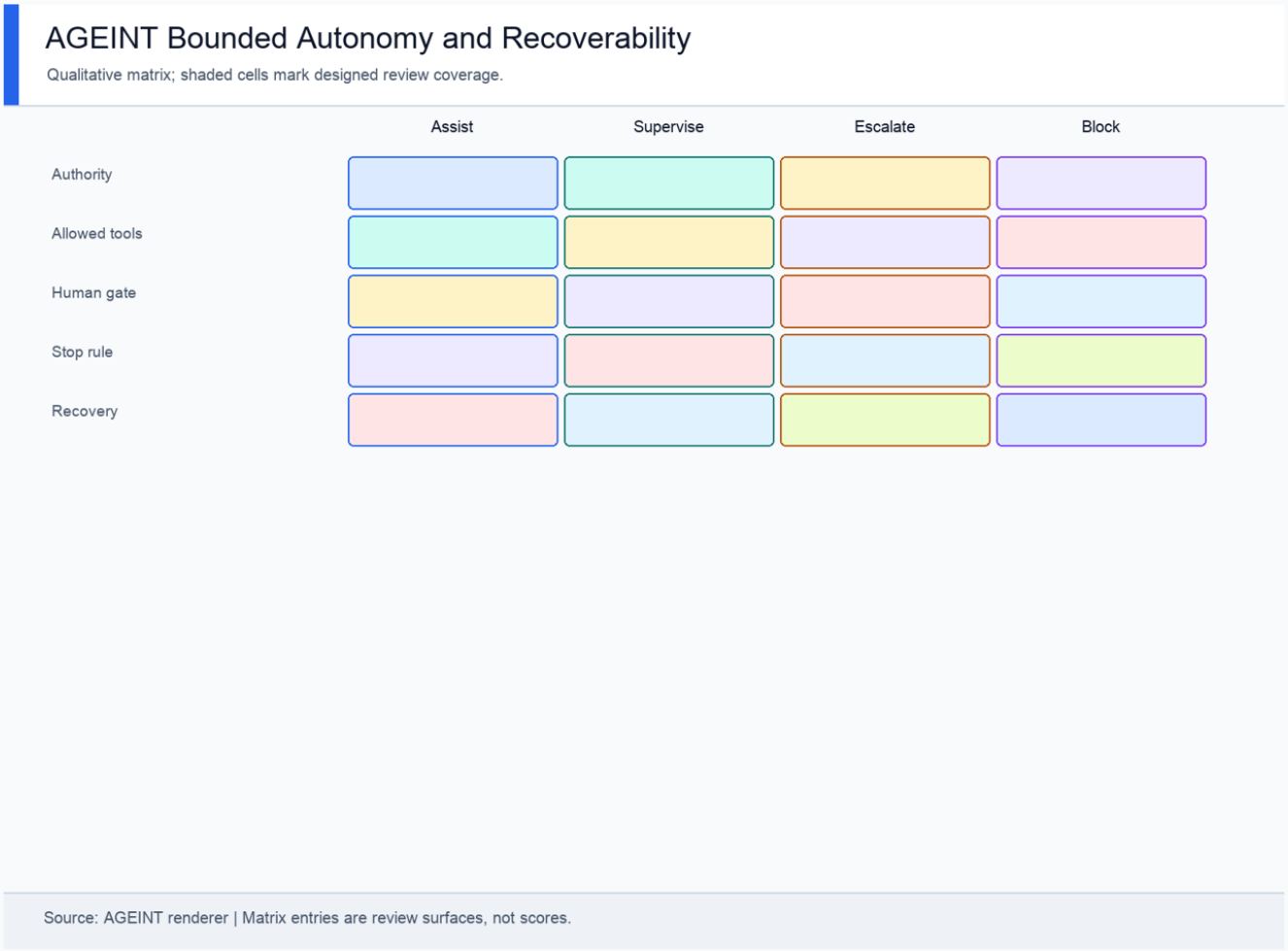


Figure 99: The bounded-autonomy view pairs delegated action with approval thresholds, stop conditions, and recovery evidence. It is anchored to the ageint agentic intelligence / ageint security and adversarial considerations section; use it to inspect bounded autonomy recoverability labels, source records, review gates, refresh cues, and reader-use boundaries while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

Figure 100: The AI incident reporting loop turns detection, classification, reporting, remediation, and learning into evidence. It is anchored to the ageint agentic intelligence / ageint security and adversarial considerations section; use it to inspect ai incident reporting loop steps, decision gates, owner handoffs, refresh triggers, and closure evidence while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

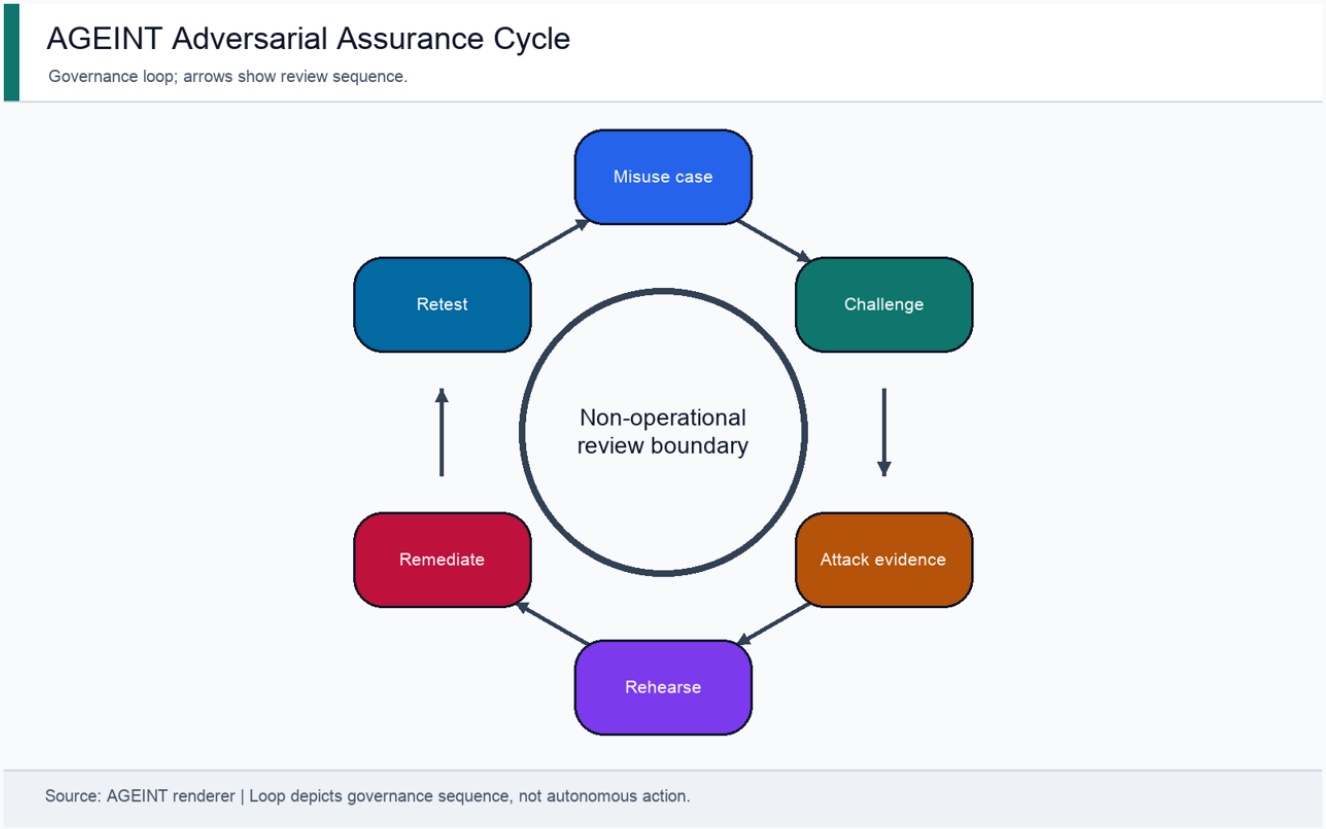


Figure 101: The adversarial assurance cycle turns misuse cases, control challenges, evidence attacks, incident rehearsal, and remediation into review evidence. Its reader value is to make adversarial assurance cycle steps, decision gates, owner handoffs, refresh triggers, and closure evidence visible at a glance, with the ageint agentic intelligence / ageint security and adversarial considerations section as the source section and defensive review as the boundary.

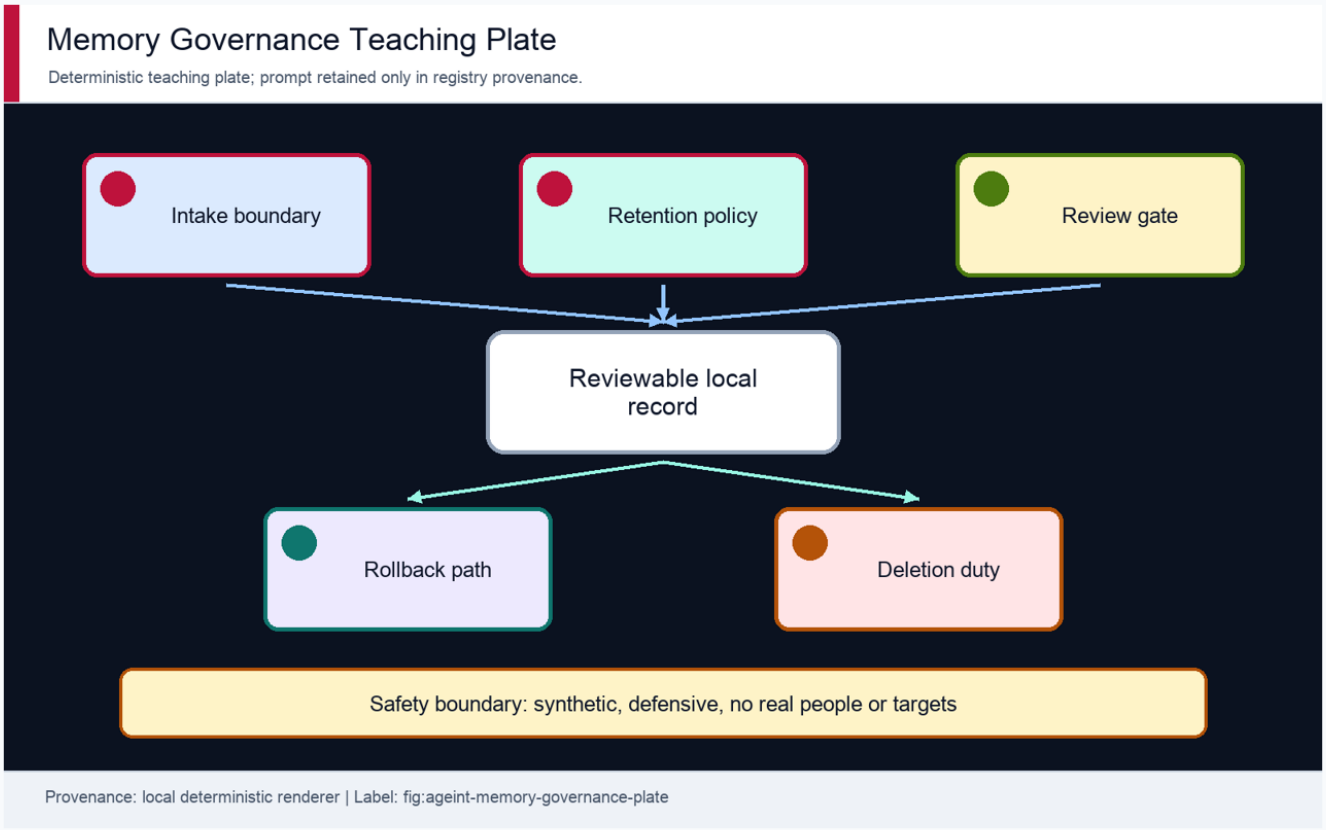


Figure 102: Deterministic teaching plate showing governed memory intake, retention, review, and rollback boundaries for AGEINT agentic assistance. Its reader value is to make Intake boundary, Retention policy, Review gate, and Rollback path visible at a glance, with the ageint agentic intelligence / ageint security and adversarial considerations section as the source section and defensive review as the boundary.

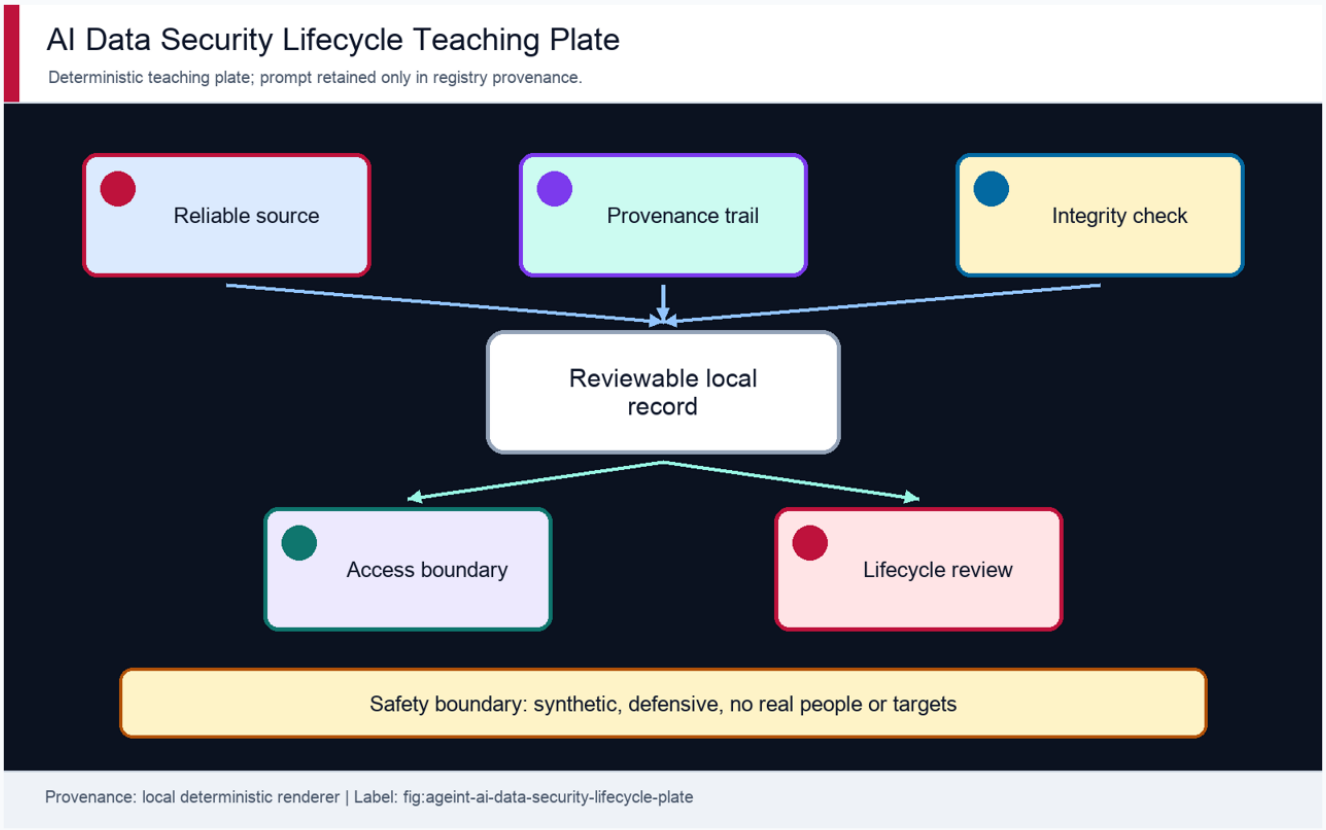


Figure 103: Deterministic teaching plate showing CISA/NSA-style AI data security as source reliability, provenance, integrity, access control, and lifecycle review. The captioned view belongs to the ageint agentic intelligence / ageint security and adversarial considerations section and should be read as a map of Reliable source, Provenance trail, Integrity check, and Access boundary, not as a capability score or live-task instruction.

48.2 Defensive Cyber-Intelligence Lens path for AGEINT Security and Adversarial Considerations: lesson cluster, safe artifact, and review

Evidence anchor. Section 48; [234, 2026].

48.2.1 AGEINT Security and Adversarial Considerations practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 48; [234, 2026].

48.2.2 AGEINT Security and Adversarial Considerations topic lessons: source-backed concepts and transfer tasks

This module builds agentic AI as delegated action under control: identity, authority, tool permissions, memory, logs, stop conditions, and recoverability define what an agent may do. The sequence opens with **Agent Framework Security Vulnerabilities**, **Python REPL sandbox and approval-gate**, **Cyber credential-and-movement taxonomy review using fabricated alerts** and applies the **Defensive Cyber-Intelligence Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 85; module overview Section 48; curriculum atlas Section 2.

Triangulation anchors. In module 34's topic-lessons section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

48.2.2.1 Lesson 1: Agent Framework Security Vulnerabilities **Concept. Agent Framework Security Vulnerabilities** treats agents as software actors with explicit permissions, logs, stop conditions, and human approval—not autonomous decision makers.

Why it matters. Without explicit treatment of **Agent Framework Security Vulnerabilities**, excessive agency undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Agent Framework Security Vulnerabilities rests on [147, 2026]. The closest source to this row notes: Security analysis of major AI agent frameworks including LangChain, CrewAI, AutoGen, Semantic. Use it for the claim that **Agent Framework Security Vulnerabilities** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Agent Framework Security Vulnerabilities**, reason from the sources cited in this row. [147, 2026] Security analysis of major AI agent frameworks including LangChain, CrewAI, AutoGen, Semantic. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. Build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this least-privilege agent design and run review topic. The artifact must name the source descriptor, the bounded claim about **Agent Framework Security Vulnerabilities**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape this subject work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that Agent Framework Security Vulnerabilities replaces human review whenever evidence looks plausible.

Transfer task. Transfer **Agent Framework Security Vulnerabilities** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

48.2.2.2 Lesson 2: Python REPL sandbox and approval-gate **Concept. Python REPL sandbox and approval-gate** evaluates agent frameworks by logging, tool allowlists, human approval, and blocked external actions—not production deployment recipes.

Why it matters. Analysts use **Python REPL sandbox** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that treating misuse taxonomy as tool permission would otherwise hide, and the reviewer accountable for challenge.

Source support. Python REPL sandbox and approval-gate rests on [299, 2026], [306, 2026], and [312, 2026]. The lead source's own note reads: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for the working definition that **Python REPL sandbox and approval-gate** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Python REPL sandbox**, reason from the sources cited in this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Python REPL sandbox**, build a blocked-request control card with tool permission, unsafe outcome, deny rule, log evidence, and reviewer disposition. Shape **Python REPL sandbox** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Python REPL sandbox**: that a misuse taxonomy describing what an autonomous agent could do is permission or a recipe to make it do so.

Transfer task. Reuse the **Python REPL sandbox** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

48.2.2.3 Lesson 3: Cyber credential-and-movement taxonomy review using fabricated alerts **Concept. Cyber credential-and-movement taxonomy review using fabricated alerts** evaluates agent frameworks by logging, tool allowlists, human approval, and blocked external actions—not production deployment recipes.

Why it matters. Analysts use **Cyber credential-and-movement taxonomy review** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that treating defensive taxonomy labels as an action sequence would otherwise hide, and the reviewer accountable for challenge.

Source support. Cyber credential-and-movement taxonomy review using fabricated alerts rests on [299, 2026], [306, 2026], and [312, 2026]. The most specific cited work observes: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for the working definition that **Cyber credential-and-movement taxonomy review using fabricated alerts** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Cyber credential-and-movement taxonomy review**, reason from the sources cited in this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Cyber credential-and-movement taxonomy review**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this least-privilege agent design and run review topic. The artifact must map the indicator descriptor, the bounded claim about **Cyber credential-and-movement taxonomy review using**, the taxonomy caveat, the confidence note, the no-action boundary, and the reviewer who validates the labeling. Shape **Cyber credential-and-movement taxonomy review** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Cyber credential-and-movement taxonomy review**: that a defensive taxonomy label is an action sequence rather than a vocabulary for describing and detecting behavior.

Transfer task. Reuse the **Cyber credential-and-movement taxonomy review** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

48.2.2.4 Lesson 4: AutoGen sandbox and code-execution approval

Concept. AutoGen sandbox and code-execution approval evaluates agent frameworks by logging, tool allowlists, human approval, and blocked external actions—not production deployment recipes.

Why it matters. AutoGen sandbox connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. AutoGen sandbox and code-execution approval rests on [147, 2026]. The lead source's own note reads: Security analysis of major AI agent frameworks including LangChain, CrewAI, AutoGen, Semantic. Use it for fixing what **AutoGen sandbox and code-execution approval** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **AutoGen sandbox**, reason from the sources cited in this row. [147, 2026] Security analysis of major AI agent frameworks including LangChain, CrewAI, AutoGen, Semantic. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **AutoGen sandbox**, build a blocked-request control card with tool permission, unsafe outcome, deny rule, log evidence, and reviewer disposition. Shape **AutoGen sandbox** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **AutoGen sandbox**: that a misuse taxonomy describing what an autonomous agent could do is permission or a recipe to make it do so.

Transfer task. Transfer **AutoGen sandbox** from this module to a second motif by preserving least-privilege agent design and run review, replacing action with audit, and naming the blocked use.

48.2.2.5 Lesson 5: MCP Server Poisoning and Prompt Injection

Concept. MCP Server Poisoning and Prompt Injection evaluates tool protocols by allowlists, logging, provenance of retrieved content, and deny-by-default policies.

Why it matters. Without explicit treatment of **MCP Server Poisoning**, excessive agency undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. MCP Server Poisoning and Prompt Injection rests on [155, 2026] and [159, 2026]. The most specific cited work observes: It identifies concerns including weak default authentication, supply-chain exposure from compromised tools, over-permissioned access tokens, injection and context-poisoning attacks, and gaps in audit logging for agentic workflows. Use them for fixing what **MCP Server Poisoning and Prompt Injection** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **MCP Server Poisoning**, work from the cited evidence behind this row. [155, 2026] Radosevich and Halloran (2025) audit security vulnerabilities in Anthropic's Model Context Protocol (MCP), which allows LLMs to integrate with external tools and data sources. The authors demonstrate that language models using MCP can be manipulated through prompt injection to execute malicious code, enable remote access, and steal credentials. [159, 2026] A September 2025 Bitdefender Business Insights article by Martin Zugec examining security risks in the Model Context Protocol, the standard introduced by Anthropic for connecting AI agents to external tools and data. It identifies concerns including weak default authentication, supply-chain exposure from compromised tools, over-permissioned access tokens, injection and context-poisoning attacks, and gaps in audit logging for agentic workflows. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **MCP Server Poisoning**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this least-privilege agent design and run review topic. The artifact must name the source descriptor, the bounded claim about **MCP Server Poisoning and Prompt**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **MCP Server Poisoning** work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that MCP Server Poisoning and Prompt Injection replaces human review whenever evidence looks plausible.

Transfer task. Transfer **MCP Server Poisoning** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

48.2.2.6 Lesson 6: Prompt Injection in Intelligence Agentic Systems

Concept. Prompt Injection in Intelligence Agentic Systems treats prompt attacks as trust-boundary failures requiring input sanitization, tool limits, and human review.

Why it matters. Prompt Injection connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Prompt Injection in Intelligence Agentic Systems rests on [137, 2026]. The lead source's own note reads: An arXiv paper surveying the shift from passive language models to Agentic AI, where large language models act as cognitive controllers that combine memory, tool use, and environmental feedback to pursue extended goals. Use it for the working definition that **Prompt Injection in Intelligence Agentic Systems** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Prompt Injection** in the evidence the row cites. [137, 2026] An arXiv paper surveying the shift from passive language models to Agentic AI, where large language models act as cognitive controllers that combine memory, tool use, and environmental feedback to pursue extended goals. It proposes a unified taxonomy organizing agent systems into six components: perception, brain, planning, action, tool use, and collaboration. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Prompt Injection**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this least-privilege agent design and run review topic. The artifact must name the source descriptor, the bounded claim about **Prompt Injection in Intelligence Agentic**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Prompt Injection** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that Prompt Injection in Intelligence Agentic Systems can be used while ignoring the rule to separate agent assistance from autonomous external action.

Transfer task. Transfer **Prompt Injection** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

48.2.2.7 Lesson 7: Hallucination in Action: When Agents Act on Fabricated Intelligence

Concept. Hallucination in Action: When Agents Act on Fabricated Intelligence applies Hallucination, in, Action within Agentic AI Governance and Tool Security: learners use separate agent assistance from autonomous external action and least-privilege agent design and run review evidence before any judgment moves forward.

Why it matters. Hallucination in Action matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; excessive agency is a common failure.

Source support. Hallucination in Action: When Agents Act on Fabricated Intelligence rests on [137, 2026]. The closest source to this row notes: An arXiv paper surveying the shift from passive language models to Agentic AI, where large language models act as cognitive controllers that combine memory, tool use, and environmental feedback to pursue extended goals. Use it for pinning down the scope of **Hallucination in Action: When Agents Act on Fabricated Intelligence**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Hallucination in Action**, work from the cited evidence behind this row. [137, 2026] An arXiv paper surveying the shift from passive language models to Agentic AI, where large language models act as cognitive controllers that combine memory, tool use, and environmental feedback to pursue extended goals. It proposes a unified taxonomy organizing agent systems into six components: perception, brain, planning, action, tool use, and collaboration. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Hallucination in Action**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this least-privilege agent design and run review topic. The artifact must name the source descriptor, the bounded claim about **Hallucination in Action**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Hallucination in Action** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that Hallucination in Action: When Agents Act on Fabricated Intelligence is optional whenever separate agent assistance from autonomous external action feels inconvenient.

Transfer task. Transfer **Hallucination in Action** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

48.2.2.8 Lesson 8: Infinite Loops and Runaway Agents: Detection and Kill Switches

Concept. Infinite Loops and Runaway Agents: Detection and Kill Switches applies Infinite, Loops, Runaway within Agentic AI Governance and Tool Security: learners use separate agent assistance from autonomous external action and least-privilege agent design and run review evidence before any judgment moves forward.

Why it matters. Infinite Loops and Runaway Agents connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Infinite Loops and Runaway Agents: Detection and Kill Switches rests on [137, 2026]. The lead source's own note reads: An arXiv paper surveying the shift from passive language models to Agentic AI, where large language models act as cognitive controllers that combine memory, tool use, and environmental feedback to pursue extended goals. Use it for the working definition that **Infinite Loops and Runaway Agents: Detection and Kill Switches** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Infinite Loops and Runaway Agents**, reason from the sources cited in this row. [137, 2026] An arXiv paper surveying the shift from passive language models to Agentic AI, where large language models act as cognitive controllers that combine memory, tool use, and environmental feedback to pursue extended goals. It proposes a unified taxonomy organizing agent systems into six components: perception, brain, planning, action, tool use, and collaboration. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Infinite Loops and Runaway Agents**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this least-privilege agent design and run review topic. The artifact must name the source descriptor, the bounded claim about **Infinite Loops and Runaway Agents**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Infinite Loops and Runaway Agents** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that Infinite Loops and Runaway Agents: Detection and Kill Switches establishes intent without reviewing alternative explanations.

Transfer task. Transfer **Infinite Loops and Runaway Agents** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

48.2.2.9 Lesson 9: Agentic AI Governance Frameworks 2026

Concept. Agentic AI Governance Frameworks 2026 — Bind AI use to purpose, evaluation, human review, rights impact, and retention before deployment in analysis.

Why it matters. Agentic AI Governance Frameworks 2026 matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; excessive agency is a common failure.

Source support. Agentic AI Governance Frameworks 2026 rests on [160, 2026] and [161, 2026]. The closest source to this row notes: The papers collectively argue that governance cannot be applied reactively after agents act but must instead be embedded at the architectural level, preventing unauthorized autonomous behavior before it occurs. Use them for the working definition that **Agentic AI Governance Frameworks 2026** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **Agentic AI Governance Frameworks 2026** against the works cited for this row. [160, 2026] Oliver Patel compiled a three-part series summarizing twelve influential research papers on governing autonomous AI systems, organized around themes of security and safety, infrastructure and principal-agent theory, and regulatory and capability assessment. The papers collectively argue that governance cannot be applied reactively after agents act but must instead be embedded at the architectural level, preventing unauthorized autonomous behavior before it occurs. [161, 2026] A January 2026 article from the law firm Davis Wright Tremaine on governance frameworks for agentic AI. It argues that autonomous, adaptive AI systems pose distinct risks, such as unauthorized or erroneous actions, biased decisions, data breaches, and opaque audit trails, that require governance beyond existing AI frameworks. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Agentic AI Governance Frameworks 2026**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this least-privilege agent design and run review topic. The artifact must name the source descriptor, the bounded claim about **Agentic AI Governance Frameworks**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape this subject work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that Agentic AI Governance Frameworks 2026 replaces human review whenever evidence looks plausible.

Transfer task. Transfer **Agentic AI Governance Frameworks 2026** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

48.2.2.10 Lesson 10: OWASP Top 10 for LLM Applications

Concept. OWASP Top 10 for LLM Applications applies OWASP, Top, LLM within Agentic AI Governance and Tool Security: learners use separate agent assistance from autonomous external action and least-privilege agent design and run review evidence before any judgment moves forward.

Why it matters. Without explicit treatment of **OWASP Top 10 for LLM Applications**, excessive agency undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. OWASP Top 10 for LLM Applications rests on [299, 2026], [306, 2026], and [312, 2026]. The lead source's own note reads: It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). Use them for pinning down the scope of **OWASP Top 10 for LLM Applications**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **OWASP Top 10 for LLM Applications**, reason from the sources cited in this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **OWASP Top 10**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this least-privilege agent design and run review topic. The artifact must name the source descriptor, the bounded claim about **OWASP Top 10 for LLM**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **OWASP Top 10 for LLM Applications** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that OWASP Top 10 for LLM Applications can be used while ignoring the rule to separate agent assistance from autonomous external action.

Transfer task. Transfer **OWASP Top 10 for LLM Applications** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

48.2.2.11 Lesson 11: IAPS Agentic AI Governance Framework

Concept. IAPS Agentic AI Governance Framework — Bind AI use to purpose, evaluation, human review, rights impact, and retention before deployment in analysis.

Why it matters. IAPS Agentic AI Governance Framework connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. IAPS Agentic AI Governance Framework rests on [299, 2026], [306, 2026], and [312, 2026]. Its anchor reference records: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for pinning down the scope of **IAPS Agentic AI Governance Framework**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **IAPS Agentic AI Governance Framework** against the works cited for this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. Build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this least-privilege agent design and run review topic. The artifact must name the source descriptor, the bounded claim about **IAPS Agentic AI Governance Framework**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape this subject work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that IAPS Agentic AI Governance Framework is optional whenever separate agent assistance from autonomous external action feels inconvenient.

Transfer task. Transfer **IAPS Agentic AI Governance Framework** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

48.2.2.12 Lesson 12: UK AI Safety Institute: Agent Evaluations

Concept. UK AI Safety Institute: Agent Evaluations treats agents as software actors with explicit permissions, logs, stop conditions, and human approval—not autonomous decision makers.

Why it matters. UK AI Safety Institute matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; excessive agency is a common failure.

Source support. UK AI Safety Institute: Agent Evaluations rests on [299, 2026], [306, 2026], and [312, 2026]. Its anchor reference records: The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. Use them for fixing what **UK AI Safety Institute: Agent Evaluations** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **UK AI Safety Institute**, work from the cited evidence behind this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **UK AI Safety Institute**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this least-privilege agent design and run review topic. The artifact must name the source descriptor,

the bounded claim about **UK AI Safety Institute**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **UK AI Safety Institute** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that UK AI Safety Institute: Agent Evaluations establishes intent without reviewing alternative explanations.

Transfer task. Transfer **UK AI Safety Institute** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

48.2.2.13 Lesson 13: LLM-agent cyber-misuse taxonomy review using sample reports **Concept. LLM-agent cyber-misuse taxonomy review using sample reports** treats agents as software actors with explicit permissions, logs, stop conditions, and human approval—not autonomous decision makers.

Why it matters. LLM-agent cyber-misuse taxonomy review connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. LLM-agent cyber-misuse taxonomy review using sample reports rests on [100, 2026]. The lead source's own note reads: This survey examines how large language model-based agents can be weaponized as autonomous cyberattack tools, analyzing their architecture across five core components: models, perception, memory, reasoning and planning, and tools. Use it for fixing what **LLM-agent cyber-misuse taxonomy review using sample reports** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **LLM-agent cyber-misuse taxonomy review** in the evidence the row cites. [100, 2026] This survey examines how large language model-based agents can be weaponized as autonomous cyberattack tools, analyzing their architecture across five core components: models, perception, memory, reasoning and planning, and tools. The authors document eight attack categories and map them across static infrastructure, mobile networks, and infrastructure-free systems such as blockchain and the metaverse. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **LLM-agent cyber-misuse taxonomy review**, build a blocked-request control card with tool permission, unsafe outcome, deny rule, log evidence, and reviewer disposition. Shape **LLM-agent cyber-misuse taxonomy review** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that a misuse taxonomy describing what an autonomous agent could do is permission or a recipe to make it do so.

Transfer task. Apply this module's safe boundary for **LLM-agent cyber-misuse taxonomy review** to another artifact while keeping least-privilege agent design and run review and reviewer ownership explicit.

48.2.2.14 Lesson 14: Threat Intelligence Gathering by LLM Agents **Concept. Threat Intelligence Gathering by LLM Agents** treats agents as software actors with explicit permissions, logs, stop conditions, and human approval—not autonomous decision makers.

Why it matters. Threat Intelligence Gathering by LLM Agents matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; excessive agency is a common failure.

Source support. Threat Intelligence Gathering by LLM Agents rests on [100, 2026]. The lead source's own note reads: The authors document eight attack categories and map them across static infrastructure, mobile networks, and infrastructure-free systems such as blockchain and the metaverse. Use it for the claim that **Threat Intelligence Gathering by LLM Agents** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Threat Intelligence Gathering by LLM Agents**, reason from the sources cited in this row. [100, 2026] This survey examines how large language model-based agents can be weaponized as autonomous cyberattack tools, analyzing their architecture across five core components: models, perception, memory, reasoning and planning, and tools. The authors document eight attack categories and map them across static infrastructure, mobile networks, and infrastructure-free systems such as blockchain and the metaverse. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Threat Intelligence Gathering by LLM Agents**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this least-privilege agent design and run review topic. The artifact must name the source descriptor, the bounded claim about **Threat Intelligence Gathering by LLM**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape this subject work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that Threat Intelligence Gathering by LLM Agents can be used while ignoring the rule to separate agent assistance from autonomous external action.

Transfer task. Transfer **Threat Intelligence Gathering by LLM Agents** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

48.2.2.15 Lesson 15: Malware-misuse control review using sample agent logs **Concept. Malware-misuse control review using sample agent logs** treats agents as software actors with explicit permissions, logs, stop conditions, and human approval—not autonomous decision makers.

Why it matters. Without explicit treatment of **Malware-misuse control review**, treating misuse taxonomy as tool permission undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Malware-misuse control review using sample agent logs rests on [100, 2026]. The most specific cited work observes: The authors document eight attack categories and map them across static infrastructure, mobile networks, and infrastructure-free systems such as blockchain and the metaverse. Use it for fixing what **Malware-misuse control review using sample agent logs** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **Malware-misuse control review** against the works cited for this row. [100, 2026] This survey examines how large language model-based agents can be weaponized as autonomous cyberattack tools, analyzing their architecture across five core components: models, perception, memory, reasoning and planning, and tools. The authors document eight attack categories and map them across static infrastructure, mobile networks, and infrastructure-free systems such as blockchain and the metaverse. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Malware-misuse control review**, build a blocked-request control card with tool permission, unsafe outcome, deny rule, log evidence, and reviewer disposition. Shape **Malware-misuse control review** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Malware-misuse control review**: that a misuse taxonomy describing what an autonomous agent could do is permission or a recipe to make it do so.

Transfer task. Reuse the **Malware-misuse control review** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

48.2.2.16 Lesson 16: Phishing-resilience control review using sample messages **Concept. Phishing-resilience control review using sample messages** teaches defensive recognition of manipulation attempts using sample messages, consent boundaries, and reporting duties.

Why it matters. Without explicit treatment of **Phishing-resilience control review**, treating misuse taxonomy as tool permission undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Phishing-resilience control review using sample messages rests on [100, 2026]. The lead source's own note reads: This survey examines how large language model-based agents can be weaponized as autonomous cyberattack tools, analyzing their architecture across five core components: models, perception, memory, reasoning and planning, and tools. Use it for fixing what **Phishing-resilience control review using sample messages** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **Phishing-resilience control review** against the works cited for this row. [100, 2026] This survey examines how large language model-based agents can be weaponized as autonomous cyberattack tools, analyzing their architecture across five core components: models, perception, memory, reasoning and planning, and tools. The authors document eight attack categories and map them across static infrastructure, mobile networks, and infrastructure-free systems such as blockchain and the metaverse. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Phishing-resilience control review**, build a blocked-request control card with tool permission, unsafe outcome, deny rule, log evidence, and reviewer disposition. Shape **Phishing-resilience control review** work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Phishing-resilience control review**: that a misuse taxonomy describing what an autonomous agent could do is permission or a recipe to make it do so.

Transfer task. Apply this module's safe boundary for **Phishing-resilience control review** to another artifact while keeping least-privilege agent design and run review and reviewer ownership explicit.

48.2.2.17 Lesson 17: Multi-agent cyber-misuse coordination review using sample reports **Concept. Multi-agent cyber-misuse coordination review using sample reports** treats agents as software actors with explicit permissions, logs, stop conditions, and human approval—not autonomous decision makers.

Why it matters. Without explicit treatment of **Multi-agent cyber-misuse coordination review**, treating misuse taxonomy as tool permission undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Multi-agent cyber-misuse coordination review using sample reports rests on [100, 2026]. The closest source to this row notes: The authors document eight attack categories and map them across static infrastructure, mobile networks, and infrastructure-free systems such as blockchain and the metaverse. Use it for fixing what **Multi-agent cyber-misuse coordination review using sample reports** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **Multi-agent cyber-misuse coordination review** in the evidence the row cites. [100, 2026] This survey examines how large language model-based agents can be weaponized as autonomous cyberattack tools, analyzing their architecture across five core components: models, perception, memory, reasoning and planning, and tools. The authors document eight attack categories and map them across static infrastructure, mobile networks, and infrastructure-free systems such as blockchain and the metaverse. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Multi-agent cyber-misuse coordination review**, build a blocked-request control card with tool permission, unsafe outcome, deny rule, log evidence, and reviewer disposition. Shape **Multi-agent cyber-misuse coordination review** work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Multi-agent cyber-misuse coordination review**: that a misuse taxonomy describing what an autonomous agent could do is permission or a recipe to make it do so.

Transfer task. Apply this module's safe boundary for **Multi-agent cyber-misuse coordination review** to another artifact while keeping least-privilege agent design and run review and reviewer ownership explicit.

48.2.2.18 Lesson 18: Networked-device cyber-misuse risk review using sample scenarios **Concept. Networked-device cyber-misuse risk review using sample scenarios** treats the topic as a misuse-case control problem: identify the agent permission, prompt path, tool boundary, and blocked outcome.

Why it matters. Networked-device cyber-misuse risk review matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; treating misuse taxonomy as tool permission is a common failure.

Source support. Networked-device cyber-misuse risk review using sample scenarios rests on [100, 2026]. Its anchor reference records: This survey examines how large language model-based agents can be weaponized as autonomous cyberattack tools, analyzing their architecture across five core components: models, perception, memory, reasoning and planning, and tools. Use it for pinning down the scope of **Networked-device cyber-misuse risk review using sample scenarios**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Networked-device cyber-misuse risk review**, work from the cited evidence behind this row. [100, 2026] This survey examines how large language model-based agents can be weaponized as autonomous cyberattack tools, analyzing their architecture across five core components: models, perception, memory, reasoning and planning, and tools. The authors document eight attack categories and map them across static infrastructure, mobile networks, and infrastructure-free systems such as blockchain and the metaverse. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Networked-device cyber-misuse risk review**, build a blocked-request control card with tool permission, unsafe outcome, deny rule, log evidence, and reviewer disposition. Shape **Networked-device cyber-misuse risk review** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Networked-device cyber-misuse risk review**: that a misuse taxonomy describing what an autonomous agent could do is permission or a recipe to make it do so.

Transfer task. Reuse the **Networked-device cyber-misuse risk review** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

48.2.2.19 Lesson 19: Observability as Control: Tracing, Logging, Audit for AGEINT Systems **Concept. Observability as Control: Tracing, Logging, Audit for AGEINT Systems** applies Observability, Control, Tracing within Agentic AI Governance and Tool Security: learners use separate agent assistance from autonomous external action and least-privilege agent design and run review evidence before any judgment moves forward.

Why it matters. Analysts use **Observability as Control** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that excessive agency would otherwise hide, and the reviewer accountable for challenge.

Source support. Observability as Control: Tracing, Logging, Audit for AGEINT Systems rests on [162, 2026]. The most specific cited work observes: It finds high adoption in IT operations alongside planned budget increases, while identifying barriers to scaling including security and compliance concerns, difficulty monitoring agents, and unclear autonomy boundaries. Use it for the working definition that **Observability as**

Control: Tracing, Logging, Audit for AGEINT Systems can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Observability as Control**, work from the cited evidence behind this row. [162, 2026] A Dynatrace blog post summarizing its Pulse of Agentic AI 2026 report, based on a survey of over 900 organizational leaders on enterprise adoption of agentic AI. It finds high adoption in IT operations alongside planned budget increases, while identifying barriers to scaling including security and compliance concerns, difficulty monitoring agents, and unclear autonomy boundaries. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Observability as Control**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this least-privilege agent design and run review topic. The artifact must name the source descriptor, the bounded claim about **Observability as Control**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Observability as Control** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that Observability as Control: Tracing, Logging, Audit for AGEINT Systems is optional whenever separate agent assistance from autonomous external action feels inconvenient.

Transfer task. Transfer **Observability as Control** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

48.2.2.20 Lesson 20: Human-in-the-Loop Architectures: When and How to Mandate Oversight

Concept. Human-in-the-Loop Architectures: When and How to Mandate Oversight applies Human, in, Loop within Agentic AI Governance and Tool Security: learners use separate agent assistance from autonomous external action and least-privilege agent design and run review evidence before any judgment moves forward.

Why it matters. Analysts use **Human-in-the-Loop Architectures** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that excessive agency would otherwise hide, and the reviewer accountable for challenge.

Source support. Human-in-the-Loop Architectures: When and How to Mandate Oversight rests on [162, 2026] and [004, 2026]. The lead source's own note reads: It finds high adoption in IT operations alongside planned budget increases, while identifying barriers to scaling including security and compliance concerns, difficulty monitoring agents, and unclear autonomy boundaries. Use them for pinning down the scope of **Human-in-the-Loop Architectures: When and How to Mandate Oversight**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **Human-in-the-Loop Architectures** against the works cited for this row. [162, 2026] A Dynatrace blog post summarizing its Pulse of Agentic AI 2026 report, based on a survey of over 900 organizational leaders on enterprise adoption of agentic AI. It finds high adoption in IT operations alongside planned budget increases, while identifying barriers to scaling including security and compliance concerns, difficulty monitoring agents, and unclear autonomy boundaries. [004, 2026] Tom Mulligan argues that artificial intelligence will enhance rather than replace human intelligence professionals, contending that the future of intelligence lies in human-machine collaboration. He maintains that uniquely human qualities such as intuition, experience, and independent judgment become more valuable as adversaries gain access to the same AI tools. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Human-in-the-Loop Architectures**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this least-privilege agent design and run review topic. The artifact must name the source descriptor, the bounded claim about **Human-in-the-Loop Architectures**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Human-in-the-Loop Architectures** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that Human-in-the-Loop Architectures: When and How to Mandate Oversight establishes intent without reviewing alternative explanations.

Transfer task. Transfer **Human-in-the-Loop Architectures** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

48.2.2.21 Lesson 21: Alignment and Trustworthiness in AGEINT: National Security Context

Concept. Alignment and Trustworthiness in AGEINT: National Security Context applies Alignment, Trustworthiness, in within Agentic AI Governance and Tool Security: learners use separate agent assistance from autonomous external action and least-privilege agent design and run review evidence before any judgment moves forward.

Why it matters. Without explicit treatment of **Alignment and Trustworthiness in AGEINT**, excessive agency undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Alignment and Trustworthiness in AGEINT: National Security Context rests on [148, 2026]. Its anchor reference records: This article by Riverside Research traces AI's evolution from large language models through retrieval-augmented systems, single-task agents, collaborative agentic systems, and toward emergent multi-agent autonomy capable of managing surveillance and decision support at operational speed. Use it for pinning down the scope of **Alignment and Trustworthiness in AGEINT: National Security Context**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Alignment and Trustworthiness in AGEINT**, reason from the sources cited in this row. [148, 2026] This article by Riverside Research traces AI's evolution from large language models through retrieval-augmented systems, single-task agents, collaborative agentic systems, and toward emergent multi-agent autonomy capable of managing surveillance and decision support at operational speed. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Alignment and Trustworthiness in AGEINT**, build a **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** for this least-privilege agent design and run review topic. The artifact must name the source descriptor, the bounded claim about **Alignment and Trustworthiness in AGEINT**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Alignment and Trustworthiness in AGEINT** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that Alignment and Trustworthiness in AGEINT: National Security Context replaces human review whenever evidence looks plausible.

Transfer task. Transfer **Alignment and Trustworthiness in AGEINT** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

48.2.3 AGEINT Security and Adversarial Considerations worked safe example: synthetic inputs, evidence, and review

Worked example: a synthetic research assistant agent organizes public readings for an instructor. [234, 2026]; [235, 2026].

Triangulation anchors. In module 34's worked-example section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **governed agentic intelligence**. Learners use a **agent run and assurance card** and keep this boundary visible: No autonomous external action, credentialed operations, live-target workflows, or uncontrolled tool use.

Frame. The classroom question centers on **Agent Framework Security Vulnerabilities**. Excluded actions stay explicit, and the **Defensive Cyber-Intelligence Lens** planning question is: Which defensive observation, confidence level, handling rule, and control implication can be stated without teaching adversary action?

Inputs. For the **Agent Framework Security Vulnerabilities** scenario, use public URLs, a fixed retrieval tool, a summarization prompt, a time budget, and a stop condition. The Defensive Cyber-Intelligence Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Agent Framework Security Vulnerabilities**, students bind the agent identity, list allowed tools, set autonomy limits, capture sources, block unsafe requests, and log approvals. Pause whenever an inference about Agent Framework Security Vulnerabilities appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Agent Framework Security Vulnerabilities** classroom scenario; unit artifact = agent run and assurance card; evidence = allowed inputs; method = least-privilege agent design and run review; output = an agent run card with tool calls, source links, blocked actions, reviewer notes, incident threshold, and recovery decision; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Agent Framework Security Vulnerabilities** as "Defensive Cyber-Intelligence Lens confirms it" is not enough. The revision ties the claim to least-privilege agent design and run review, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Agent Framework Security Vulnerabilities** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

48.2.4 AGEINT Security and Adversarial Considerations practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Defensive Cyber-Intelligence Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**.

Triangulation anchors. In module 34's practice-sequence section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Agent Framework Security Vulnerabilities, Python REPL sandbox and approval-gate, Cyber credential-and-movement taxonomy review using fabricated alerts; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Agentic AI Governance and Tool Security** lane.
2. Frame	Answer the lens question: Which defensive observation, confidence level, handling rule, and control implication can be stated without teaching adversary action?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Agent Framework Security Vulnerabilities: defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the agent run and assurance card fields for Agent Framework Security Vulnerabilities.	Unit profile note.	Evidence artifacts include tool-allowlist record, external-memory governance boundary.
4. Challenge	Test the misconception that Agent Framework Security Vulnerabilities replaces human review whenever evidence looks plausible.	Failure-mode note.	The artifact applies the key distinction: separate agent assistance from autonomous external action.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

48.2.4.1 AGEINT Security and Adversarial Considerations instructor notes: source reasoning, review points, and studio focus

Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**. [234, 2026]; [235, 2026].

48.2.4.2 AGEINT Security and Adversarial Considerations extension exercise: peer validation and refresh trigger review Evidence anchor.

Section 48; [234, 2026].

Have learners swap artifacts and apply the **Defensive Cyber-Intelligence Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**.

48.2.5 AGEINT Security and Adversarial Considerations knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 48; [234, 2026].

1. Explain how **Agent Framework Security Vulnerabilities** is defined here; name the source descriptor that supports the definition.
2. Contrast **Agent Framework Security Vulnerabilities** with **Python REPL sandbox and approval-gate** using the **Defensive Cyber-Intelligence Lens** artifact fields.
3. Identify one failure mode from the **Agentic AI Governance and Tool Security** lane and the evidence that would reveal it.

4. Answer the coursebook review question: Which permission can be removed while preserving the learning objective?
5. Correct this misconception: that Agent Framework Security Vulnerabilities replaces human review whenever evidence looks plausible.

48.2.5.1 AGEINT Security and Adversarial Considerations answer quality rubric: source evidence, uncertainty, and safe transfer

Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Agent Framework Security Vulnerabilities** without source evidence, uncertainty, or a safe transfer task.

48.3 AGEINT Security and Adversarial Considerations assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 48; [234, 2026].

48.3.1 AGEINT Security and Adversarial Considerations evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 48; [234, 2026].

48.3.2 AGEINT Security and Adversarial Considerations transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 48; [234, 2026].

48.3.2.1 AGEINT Security and Adversarial Considerations lineage and source tradition: profile, concepts, and first anchors This sits in the **Agentic AI Governance and Tool Security** lineage: delegated action under explicit authority, identity, permissions, tool boundaries, monitoring, and human escalation. [234, 2026]; [235, 2026].

48.3.2.2 AGEINT Security and Adversarial Considerations working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 48; [234, 2026].
The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**, with provenance and reviewability throughout.

48.3.2.3 AGEINT Security and Adversarial Considerations knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [234, 2026]; [235, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

48.3.2.4 AGEINT Security and Adversarial Considerations transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 48; [234, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**.
- **Evidence contract:** keep the **Agentic AI Governance and Tool Security** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

48.3.2.5 AGEINT Security and Adversarial Considerations profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 48; [234, 2026].
The matched profile emphasizes delegated action under explicit authority, identity, permissions, tool boundaries, monitoring, and human escalation. The method stack is AI RMF Govern-Map-Measure-Manage, least-privilege tool design, prompt-injection review, progressive deployment, and rollback drills; the local topic cluster is **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**.

48.3.3 AGEINT Security and Adversarial Considerations evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 48; [234, 2026].
Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Agentic AI Governance and Tool Security** profile tells reviewers what evidence is strong enough for the module artifact built around **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**.

48.3.3.1 AGEINT Security and Adversarial Considerations guide source spine: inherited keys and local citation roles Primary guide citations: [234, 2026]; [235, 2026]; [236, 2026]; [276, 2026]; [277, 2026]; [284, 2026]; [288, 2026]; [289, 2026]; [293, 2026]; [147, 2026]; [155, 2026]; [159, 2026]; [137, 2026]; [160, 2026]; [161, 2026]; [100, 2026]; [162, 2026]; [004, 2026]; [148, 2026]; [299, 2026]; [306, 2026]; [312, 2026].

48.3.3.2 AGEINT Security and Adversarial Considerations verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [234, 2026]; [235, 2026].

Tier	What counts	How it is used
Source guide	[234, 2026]; [235, 2026]; [236, 2026]; [276, 2026]; [277, 2026]; [284, 2026]; [288, 2026]; [289, 2026]; [293, 2026]; [147, 2026]; [155, 2026]; [159, 2026]; [137, 2026]; [160, 2026]; [161, 2026]; [100, 2026]; [162, 2026]; [004, 2026]; [148, 2026]; [299, 2026]; [306, 2026]; [312, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 34's source-canon section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Maintenance rule: Perplexity may suggest candidates for **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate** and [234, 2026]; [235, 2026], but only directly verified source URLs are encoded as citations.

48.3.3.3 AGEINT Security and Adversarial Considerations intelligence practice lens: evidence artifact and safety check Practice lens: **Agentic Tool-Governance Lens** for **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**. [234, 2026]; [235, 2026].

Planning question: Which human authority, agent identity, tool permission, autonomy limit, incident threshold, and recoverability condition bounds the workflow?

Evidence artifact: agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path.

Validation rule: verify least privilege, prompt-injection exposure, provenance, observability, stop conditions, and incident-reporting triggers. Applied to **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**.

Handoff contract: export agent traces, tool calls, retrieved sources, policy decisions, and human approvals separately.

Safety check: block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions.

48.3.3.4 AGEINT Security and Adversarial Considerations runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 48; [234, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	34.99	34.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind AGEINT Security and Adversarial Considerations to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
AGEINT pattern registry, agent identity, and interface-contract studio	34.100	34.100 source title transformed into safe curriculum treatment; original: V2 AGEINT-depth extension: require compliance mapping, adversarial evaluation, impact assessment, trustworthiness review, and accountable remediation for agent security discussions	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Bounded autonomy, procurement, incident-response, and assurance studio	34.101	34.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for AGEINT Security and Adversarial Considerations	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Model-card, recoverability, retention, and learner-support evidence package	34.102	34.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for AGEINT Security and Adversarial Considerations	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Agent Framework Security Vulnerabilities	34.1	34.1 Agent Framework Security Vulnerabilities	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Python REPL sandbox and approval-gate	34.1.1	34.1.1 source title transformed into safe curriculum treatment; original: LangChain PythonREPLTool: Arbitrary Code Execution	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Cyber credential-and-movement taxonomy review using fabricated alerts	34.1.2	34.1.2 source title transformed into safe curriculum treatment; original: CrewAI Uncontrolled Lateral Movement Between Agents	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
AutoGen sandbox and code-execution approval	34.1.3	34.1.3 source title transformed into safe curriculum treatment; original: AutoGen Unsandboxed Code Execution	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
MCP Server Poisoning and Prompt Injection	34.1.4	34.1.4 MCP Server Poisoning and Prompt Injection	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Prompt Injection in Intelligence Agentic Systems	34.2	34.2 Prompt Injection in Intelligence Agentic Systems	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Hallucination in Action: When Agents Act on Fabricated Intelligence	34.3	34.3 Hallucination in Action: When Agents Act on Fabricated Intelligence	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Infinite Loops and Runaway Agents: Detection and Kill Switches	34.4	34.4 Infinite Loops and Runaway Agents: Detection and Kill Switches	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Agentic AI Governance Frameworks 2026	34.5	34.5 Agentic AI Governance Frameworks 2026	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
OWASP Top 10 for LLM Applications	34.5.1	34.5.1 OWASP Top 10 for LLM Applications	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
IAPS Agentic AI Governance Framework	34.5.2	34.5.2 IAPS Agentic AI Governance Framework	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
UK AI Safety Institute: Agent Evaluations	34.5.3	34.5.3 UK AI Safety Institute: Agent Evaluations	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
LLM-agent cyber-misuse taxonomy review using sample reports	34.6	34.6 source title transformed into safe curriculum treatment; original: LLM-Based Agents in Autonomous Cyberattacks: Survey and Taxonomy	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Threat Intelligence Gathering by LLM Agents	34.6.1	34.6.1 Threat Intelligence Gathering by LLM Agents	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Malware-misuse control review using sample agent logs	34.6.2	34.6.2 source title transformed into safe curriculum treatment; original: Automated Weaponization: Malware Generation	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Phishing-resilience control review using sample messages	34.6.3	34.6.3 source title transformed into safe curriculum treatment; original: Phishing and Spear-Phishing Automation	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Multi-agent cyber-misuse coordination review using sample reports	34.6.4	34.6.4 source title transformed into safe curriculum treatment; original: Multi-Agent Collaboration in Cyberattacks	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Networked-device cyber-misuse risk review using sample scenarios	34.6.5	34.6.5 source title transformed into safe curriculum treatment; original: Cyberattack Capabilities Across 6G, IoT, Satellite, UAV Networks	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Observability as Control: Tracing, Logging, Audit for AGEINT Systems	34.7	34.7 Observability as Control: Tracing, Logging, Audit for AGEINT Systems	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Human-in-the-Loop Architectures: When and How to Mandate Oversight	34.8	34.8 Human-in-the-Loop Architectures: When and How to Mandate Oversight	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Alignment and Trustworthiness in AGEINT: National Security Context	34.9	34.9 Alignment and Trustworthiness in AGEINT: National Security Context	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

48.3.3.5 AGEINT Security and Adversarial Considerations reusable subsection contract: topic rows, artifacts, and safety duties Evidence anchor. Section 48; [234, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Agent Framework Security Vulnerabilities	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Python REPL sandbox and approval-gate	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Cyber credential-and-movement taxonomy review using fabricated alerts	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
AutoGen sandbox and code-execution approval	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
MCP Server Poisoning and Prompt Injection	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Prompt Injection in Intelligence Agentic Systems	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Hallucination in Action: When Agents Act on Fabricated Intelligence	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Infinite Loops and Runaway Agents: Detection and Kill Switches	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Agentic AI Governance Frameworks 2026	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
OWASP Top 10 for LLM Applications	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
IAPS Agentic AI Governance Framework	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
UK AI Safety Institute: Agent Evaluations	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
LLM-agent cyber-misuse taxonomy review using sample reports	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Threat Intelligence Gathering by LLM Agents	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Malware-misuse control review using sample agent logs	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Phishing-resilience control review using sample messages	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Multi-agent cyber-misuse coordination review using sample reports	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Networked-device cyber-misuse risk review using sample scenarios	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Observability as Control: Tracing, Logging, Audit for AGEINT Systems	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Human-in-the-Loop Architectures: When and How to Mandate Oversight	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

Lesson topic	Practice lens	Evidence artifact	Safety check
Alignment and Trustworthiness in AGEINT: National Security Context	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

48.3.3.6 AGEINT Security and Adversarial Considerations annotated source ledger: real titles and local contribution Each source cited by this **Agentic AI Governance and Tool Security** module is paired below with its real title and a one-line note on what it contributes to **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**.

Source	Cited work	What it contributes	Status
[234, 2026]	AI Act	The European Commission's official page on the AI Act, described as the first comprehensive legal framework on artificial intelligence worldwide. It explains the regulation's risk-based approach, classifying AI systems into unacceptable, high, transparency, and minimal risk tiers, with prohibited practices and strict requirements for high-risk uses.	verified source-guide
[235, 2026]	ISO/IEC 42005:2025 AI System Impact Assessment	ISO standard page for AI system impact assessment.	original source-guide
[236, 2026]	ISO/IEC TR 24028:2020 Artificial Intelligence Trustworthiness Overview	The ISO catalog page for ISO/IEC TR 24028:2020, a technical report titled "Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence." The document surveys topics related to AI trustworthiness, including approaches to establishing trust through transparency, explainability, and controllability, and approaches to assess and achieve availability, resilience, reliability, accuracy, safety, security, and privacy of AI systems.	verified source-guide
[276, 2026]	What is a Data Protection Impact Assessment and When Is This Mandatory?	A European Data Protection Board FAQ page, part of its data protection guide for small businesses, explaining Data Protection Impact Assessments (DPIAs) and when they are mandatory. It describes a DPIA as a written assessment of the impact of a planned processing operation, required when processing poses high risks to individuals' rights.	verified source-guide
[277, 2026]	Endorsed WP29 Guidelines	This is a European Data Protection Board webpage listing guidelines and documents originating from the Article 29 Working Party that the EDPB endorsed at its first plenary meeting. The catalogued materials relate to the GDPR and cover topics such as consent and transparency, data breach notification, automated decision-making and profiling, data protection impact assessments, data protection officers, and binding corporate rules.	verified source-guide

Source	Cited work	What it contributes	Status
[284, 2026]	Verifiable Credential Data Integrity 1.0	The W3C Recommendation for Verifiable Credential Data Integrity 1.0, published May 2025, defining mechanisms for ensuring the authenticity and integrity of verifiable credentials using cryptographic proofs. It specifies a process of data transformation, hashing, and proof generation, and a corresponding verification procedure, along with a proof data model containing properties such as type, verification method, purpose, and proof value.	verified source-guide
[288, 2026]	Algorithmic Transparency Recording Standard Hub	A GOV.UK collection page serving as the hub for the UK Algorithmic Transparency Recording Standard (ATRS), maintained by the Government Digital Service. It provides a standardized template for documenting public-sector use of algorithmic tools, completion guidance, policy on scope and compliance, and a searchable repository of published transparency records.	verified source-guide
[289, 2026]	Guidance for Organisations Using the Algorithmic Transparency Recording Standard	This is a GOV.UK guidance page published by the Government Digital Service that instructs public sector organizations on completing the Algorithmic Transparency Recording Standard (ATRS) template and publishing their records to the GOV.UK repository. It applies both to central government bodies required to publish under mandatory policy and to other public sector bodies doing so voluntarily.	verified source-guide
[293, 2026]	Inventory of NARA Artificial Intelligence (AI) Use Cases	The National Archives and Records Administration (NARA) official inventory of its artificial intelligence use cases, documenting 14 projects across deployed, pilot, and planned stages. Deployed efforts include workplace productivity tools, automated tagging for museum experiences, and historical record retrieval, while pilots cover PII detection and redaction, semantic search, and metadata generation, and planned work targets FOIA processing and public search.	verified source-guide
[147, 2026]	Agent Framework Security	Security analysis of major AI agent frameworks including LangChain, CrewAI, AutoGen, Semantic.	original practitioner context; secondary evidence only
[155, 2026]	Model Context Protocol (MCP): Security Design Considerations	Radosevich and Halloran (2025) audit security vulnerabilities in Anthropic's Model Context Protocol (MCP), which allows LLMs to integrate with external tools and data sources. The authors demonstrate that language models using MCP can be manipulated through prompt injection to execute malicious code, enable remote access, and steal credentials.	verified source-guide

Source	Cited work	What it contributes	Status
[159, 2026]	Security Risks of Agentic AI: A Model Context Protocol (MCP	A September 2025 Bitdefender Business Insights article by Martin Zugec examining security risks in the Model Context Protocol, the standard introduced by Anthropic for connecting AI agents to external tools and data. It identifies concerns including weak default authentication, supply-chain exposure from compromised tools, over-permissioned access tokens, injection and context-poisoning attacks, and gaps in audit logging for agentic workflows.	verified practitioner context; secondary evidence only
[137, 2026]	[2601.12560] Agentic Artificial Intelligence (AI)	An arXiv paper surveying the shift from passive language models to Agentic AI, where large language models act as cognitive controllers that combine memory, tool use, and environmental feedback to pursue extended goals. It proposes a unified taxonomy organizing agent systems into six components: perception, brain, planning, action, tool use, and collaboration.	verified source-guide
[160, 2026]	Breaking down the Top 12 Papers on Agentic AI Governance	Oliver Patel compiled a three-part series summarizing twelve influential research papers on governing autonomous AI systems, organized around themes of security and safety, infrastructure and principal-agent theory, and regulatory and capability assessment. The papers collectively argue that governance cannot be applied reactively after agents act but must instead be embedded at the architectural level, preventing unauthorized autonomous behavior before it occurs.	verified practitioner context; secondary evidence only
[161, 2026]	New Governance Frameworks Offer a Roadmap for Managing Risks	A January 2026 article from the law firm Davis Wright Tremaine on governance frameworks for agentic AI. It argues that autonomous, adaptive AI systems pose distinct risks, such as unauthorized or erroneous actions, biased decisions, data breaches, and opaque audit trails, that require governance beyond existing AI frameworks.	verified source-guide
[100, 2026]	A Survey on Large Language Model-based Agents in Autonomous	This survey examines how large language model-based agents can be weaponized as autonomous cyberattack tools, analyzing their architecture across five core components: models, perception, memory, reasoning and planning, and tools. The authors document eight attack categories and map them across static infrastructure, mobile networks, and infrastructure-free systems such as blockchain and the metaverse.	verified source-guide
[162, 2026]	Agentic AI report reveals need for reliable autonomous operations	A Dynatrace blog post summarizing its Pulse of Agentic AI 2026 report, based on a survey of over 900 organizational leaders on enterprise adoption of agentic AI. It finds high adoption in IT operations alongside planned budget increases, while identifying barriers to scaling including security and compliance concerns, difficulty monitoring agents, and unclear autonomy boundaries.	verified source-guide

Source	Cited work	What it contributes	Status
[004, 2026]	AI Won't Replace Spies—It Will Make Them More Powerful Than Ever	Tom Mulligan argues that artificial intelligence will enhance rather than replace human intelligence professionals, contending that the future of intelligence lies in human-machine collaboration. He maintains that uniquely human qualities such as intuition, experience, and independent judgment become more valuable as adversaries gain access to the same AI tools.	verified source-guide
[148, 2026]	How Riverside Research Advances Agentic AI for National Security	This article by Riverside Research traces AI's evolution from large language models through retrieval-augmented systems, single-task agents, collaborative agentic systems, and toward emergent multi-agent autonomy capable of managing surveillance and decision support at operational speed.	verified source-guide
[299, 2026]	Model Context Protocol Specification	The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation).	verified source-guide context; use pinned MCP anchor for normative claims
[306, 2026]	Artificial Intelligence	Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support.	original source-guide
[312, 2026]	Guide on the Use of Agentic Artificial Intelligence	Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support.	original source-guide

Where this sits. This module's overview is Section 48; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

48.3.4 AGEINT Security and Adversarial Considerations governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 48; [234, 2026].

48.3.5 AGEINT Security and Adversarial Considerations analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 34's governance-boundary section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **Agentic AI Governance and Tool Security** for **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**. [234, 2026]; [235, 2026].

Curriculum topic spine: Agent Framework Security Vulnerabilities, **Python REPL sandbox and approval-gate**, **Cyber credential-and-movement taxonomy review using fabricated alerts**. **Verified anchor cluster:** [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]; [Community, 2020b]; [Community, 2020a]; [of the Director of National Intelligence, 2025b].

Conceptual depth: delegated action under explicit authority, identity, permissions, tool boundaries, monitoring, and human escalation.

Method stack: AI RMF Govern-Map-Measure-Manage, least-privilege tool design, prompt-injection review, progressive deployment, and rollback drills.

Composability contract: agents, tools, credentials, memory, retrieval stores, policies, and logs remain separately inspectable and revocable components.

Known failure modes: excessive agency, shadow tools, indirect prompt injection, memory poisoning, confused authority, and unbounded action chains.

Defensive boundary: agentic workflows stay synthetic, owned-lab, supervised, logged, rate-limited, and reversible unless a lawful production authority exists. Applied to **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**.

Anchor	Why it matters here
[OECD, 2026a]	Official OECD conceptual foundation for agentic AI. Checked as of 2026-05-21; role: source_quality_anchor.
[of Canada Secretariat, 2026a]	Government of Canada guide for accountable public-sector use of agentic AI, including governance, risk, transparency, testing, monitoring, and human oversight considerations. Checked as of 2026-05-24; role: curriculum_anchor.
[of Standards and Technology, 2023]	Official NIST.AI.100-1 risk-management framework. Checked as of 2026-05-21; role: source_quality_anchor.
[of Standards and Technology, 2024d]	Official NIST AI 600-1 generative AI profile. Checked as of 2026-05-21; role: source_quality_anchor.
[Community, 2020b]	Official IC principles for lawful, accountable, objective, human-centered, secure, resilient, and science-informed AI. Checked as of 2026-05-21; role: curriculum_anchor.
[Community, 2020a]	Official IC framework for AI goals, authorities, human judgment, bias mitigation, testing, documentation, explainability, and review. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2025b]	Official IC AI governance directive covering CAIO roles, oversight, interoperability, civil-liberties review, training data, and impact assessment. Checked as of 2026-05-21; role: curriculum_anchor.

48.3.5.1 Threat-model framework: MAESTRO seven layers The CSA MAESTRO model gives a concrete map of where an agentic system can be attacked, shown in Figure 92. It stacks seven layers of the agent lifecycle: foundation models (L1: adversarial examples, model stealing, backdoors), data operations (L2: poisoning, RAG-pipeline compromise), agent frameworks (L3: supply chain and input validation), deployment and infrastructure (L4: container escape, lateral movement), evaluation and observability (L5: metric manipulation, detection evasion), and the agent ecosystem (L7: impersonation, marketplace and goal manipulation). The layer that carries the sharpest lesson is L6, Security and Compliance, which is drawn cross-cutting every other layer rather than stacked among them: the security agents you deploy to watch the system are themselves an attack surface, so a mature design must monitor the monitors [Alliance, 2025b]; [Initiative), 2025].

48.3.5.2 Governance control: SRE circuit breaker Knowing where attacks land is not the same as bounding their blast radius. The SRE circuit-breaker teaching pattern, depicted in Figure 93, adapts reliability vocabulary into an author-defined governance exercise for agents with three states. In CLOSED the agent operates normally, its autonomy earned by a clean safety record; when the safety error budget is exhausted – for this curriculum, when the PolicyCompliance service-level indicator falls below 99 percent – the breaker trips to OPEN and a human takes over; after a recovery period plus validation it moves to HALF_OPEN with limited capability, returning to CLOSED only if the clean record holds and snapping back to OPEN on any new violation. Activation triggers include policy-bypass attempts, LLM-provider errors, tool-timeout cascades, trust-score degradation, and reasoning loops or deadlocks. Teach this as a defensive governance exercise: define the PolicyCompliance SLI for a synthetic agent, set its error budget, and rehearse the OPEN-state human takeover as a tabletop rather than a live intervention [arXiv preprint authors, 2025b]; [United Nations University, 2026].

The PolicyCompliance service-level indicator makes the 99-percent threshold concrete. Over a review window of N_{total} governed actions with $N_{\text{violations}}$ policy violations, define

$$\text{PolicyCompliance}_{\text{SLI}} = \frac{N_{\text{total}} - N_{\text{violations}}}{N_{\text{total}}} \;\geq\; 0.99,$$

so the breaker's CLOSED state is exactly the region where this indicator clears its target. The complementary error budget is the count of violations the window can absorb before the indicator drops below target,

$$\text{ErrorBudget} = (1 - 0.99)\, N_{\text{total}} = 0.01\, N_{\text{total}}, \qquad \text{breaker} \to \text{OPEN when } N_{\text{violations}} > \text{ErrorBudget}.$$

The budget burns down as violations accrue and is restored when a fresh window opens, which is the quantity the safety-error-budget figure tracks. Have students compute the SLI on a synthetic action log, set N_{total} for one window, and identify the exact violation count that trips the breaker [arXiv preprint authors, 2025b].

48.3.5.3 AGEINT Security and Adversarial Considerations evidence standard and citation floor: source families and discovery limits Official guidance supplies governance, safety, and legal constraints for the **Agentic AI Governance and Tool Security** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [234, 2026]; [235, 2026].

48.3.6 AGEINT Security and Adversarial Considerations agentic boundary: assist, approve, block, and record

Evidence anchor. Section 48; [234, 2026].

AGEINT translation is bounded by the **Agentic AI Governance and Tool Security** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**.

48.3.6.1 AGEINT Security and Adversarial Considerations permitted defensive utility: curriculum uses and safe outputs Evidence anchor. Section 48; [234, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**.

48.3.6.2 AGEINT Security and Adversarial Considerations excluded operational boundary: blocked actions and stop rules Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [234, 2026]; [235, 2026] and **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

48.3.7 AGEINT Security and Adversarial Considerations governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 48; [234, 2026].

Governance is practiced as a gate on the **Agentic AI Governance and Tool Security** lane. Learners use the **Defensive Cyber-Intelligence Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**.

48.3.7.1 AGEINT Security and Adversarial Considerations governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [234, 2026]; [235, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Agentic AI Governance and Tool Security** failure modes and the **Defensive Cyber-Intelligence Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

48.3.7.2 AGEINT Security and Adversarial Considerations evidence package handoff: appendices, records, and reuse Evidence anchor. Section 48; [234, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Defensive Cyber-Intelligence Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**.

48.3.7.3 AGEINT Security and Adversarial Considerations current-source assurance: verified anchors and local artifact fit The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**. [234, 2026]; [235, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_oecd_agentic_ai` for **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**?	The Agentic AI Landscape and Its Conceptual Foundations; lane `source_quality_spine`; checked 2026-05-21.	defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication; Official OECD conceptual foundation for agentic AI.
What does the module inherit from `official_canada_agentic_ai_guide` for **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**?	Guide on the Use of Agentic Artificial Intelligence; lane `public_sector_agentic_ai`; checked 2026-05-24.	defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication; bounded-autonomy run card, recoverability review, approval threshold, monitoring evidence, and public-sector service assurance
What does the module inherit from `official_nist_ai_rmf` for **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**?	Artificial Intelligence Risk Management Framework (AI RMF 1.0); lane `source_quality_spine`; checked 2026-05-21.	defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication; Official NIST.AI.100-1 risk-management framework.

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_nist_ai_600_1` for **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**?	Artificial Intelligence Risk Management Framework: Generative AI Profile; lane `source_quality_spine`; checked 2026-05-21.	defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication; Official NIST AI 600-1 generative AI profile.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 48; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

48.3.8 AGEINT Security and Adversarial Considerations assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 48; [234, 2026].

48.3.9 AGEINT Security and Adversarial Considerations assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 48; [234, 2026].

48.3.9.1 AGEINT Security and Adversarial Considerations capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate** and [234, 2026]; [235, 2026].

48.3.9.2 AGEINT Security and Adversarial Considerations instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate** and [234, 2026]; [235, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

48.3.9.3 AGEINT Security and Adversarial Considerations assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Agent Framework Security Vulnerabilities	Completed **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Python REPL sandbox and approval-gate	Completed **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Cyber credential-and-movement taxonomy review using fabricated alerts	Completed **defensive CTI packet with indicator context, taxonomy mapping, confidence, handling rule, and control implication** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

48.3.10 AGEINT Security and Adversarial Considerations refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [234, 2026]; [235, 2026] and **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**.

48.3.10.1 AGEINT Security and Adversarial Considerations refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**. The local signals begin with [234, 2026]; [235, 2026].

48.3.10.2 AGEINT Security and Adversarial Considerations claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**, and the source spine for these checks begins with [234, 2026]; [235, 2026].

48.3.11 AGEINT Security and Adversarial Considerations reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [234, 2026]; [235, 2026].

Triangulation anchors. In module 34's review-checklist section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate**. [234, 2026]; [235, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

48.3.12 AGEINT Security and Adversarial Considerations learning-path links: module map, overview, and curriculum atlas

Use the cross-links below to place **Agent Framework Security Vulnerabilities; Python REPL sandbox and approval-gate** in the wider unit: the orientation sets the frame, the parent unit supplies the shared safety posture, and the neighbouring modules show what evidence enters and leaves. Lead sources: [234, 2026]; [235, 2026].

Section 2, Section 44, Section 47, Section 49

49 Active Inference and AGEINT

49.0.1 Active Inference and AGEINT figures and course links: visual evidence, source flow, and navigation

The module uses Figure 104, Figure 105, and Figure 85 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 44, Section 48, Section 50.
This module teaches the **Active-Inference Theory and Governed Agent Analogy** lane through a bounded, source-backed coursebook chapter. [247, 2026]; [248, 2026].

49.1 Active-Inference Theory and Governed Agent Analogy frame for Active Inference and AGEINT: source context, topic focus, and reader task

Evidence anchor. Section 49; [247, 2026].

49.1.1 Active Inference and AGEINT orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 49; [247, 2026].

49.1.2 Active Inference and AGEINT conceptual primer: source context, core model, and reader task

This chapter teaches agentic AI as delegated action under control: identity, authority, tool permissions, memory, logs, stop conditions, and recoverability define what an agent may do. The chapter uses **Active-Inference Boundary Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**.
The central distinction is to separate agent assistance from autonomous external action. Core topics include **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior; Shared Protentions in Multi-Agent Active Inference**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Friston, 2010]; [Christopher L. Buckley and Seth, 2017]; [Friston, 2017]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [247, 2026]; [248, 2026].
Learners move from vocabulary and the **Active-Inference Boundary Lens** distinction through topic lessons on **The Free Energy Principle and Predictive Processing** with evidence and misconception checks, then assemble a **theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition** with safety and rights gates.

49.1.3 Active Inference and AGEINT learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 49; [247, 2026].

- Connect **The Free Energy Principle and Predictive Processing and Active Inference as Computational Model of Intelligence Agent Behavior** to **Active-Inference Theory and Governed Agent Analogy** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate agent assistance from autonomous external action; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as treating a formal theory as product evidence, using analogy as architecture proof, citing policy guidance for mathematical claims, and letting autonomy language outrun evaluation evidence, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: active-inference material stays theoretical and classroom bounded; it does not prove autonomous action, intent detection, operational performance, or deployment without explicit authority and review.

49.1.4 Active Inference and AGEINT core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 49; [247, 2026].

Term	Working definition
Agent identity	the named software actor, role, and authorization context for a run
Tool allowlist	the bounded set of actions the agent may request
Delegation	the handoff of a task under explicit human authority and review
Bounded autonomy	the documented ceiling on what an agent may decide or request without review
Recoverability	the path back to a known-safe state after a bad output or action request
AI incident	a logged event where an AI system creates or plausibly creates harm or loss of control
Prompt injection	untrusted content that attempts to override instructions or authority boundaries
Pattern registry	the catalog of approved agent behaviors, prompts, and evaluation hooks
Adversarial eval	structured tests that probe agent misuse, injection, and over-delegation before release
The Free Energy Principle and Predictive…	Key terms: Free, Energy, Principle.
Active Inference as Computational Model of…	Key terms: Active, Inference, Computational.

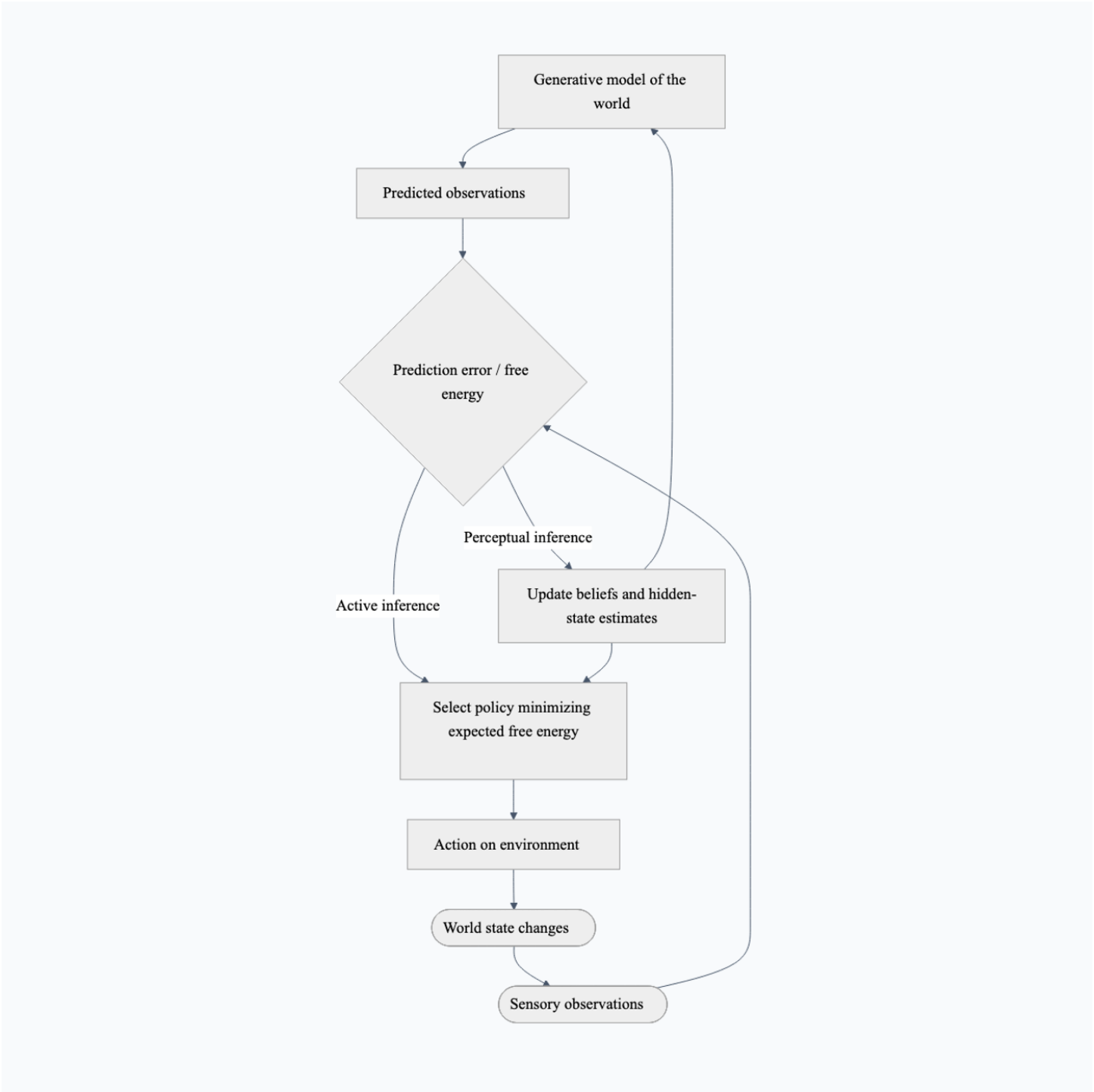


Figure 104: Conceptual teaching schematic for one active-inference interpretation of perception, belief updating, policy selection, and action; it is not validated AGEINT agent architecture or proof of autonomous performance. It is anchored to the ageint agentic intelligence / active inference and ageint section; use it to inspect A . A generative model produces predictions, which are compared against sensory observations to compute prediction error or free energy. The error branches to perceptual inference that updates beliefs, to policy selection that may choose an action, and with a governance caveat that the schematic is a theory analogy rather than deployment evidence. teaching schematic for one active-inference interpretation of perception while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

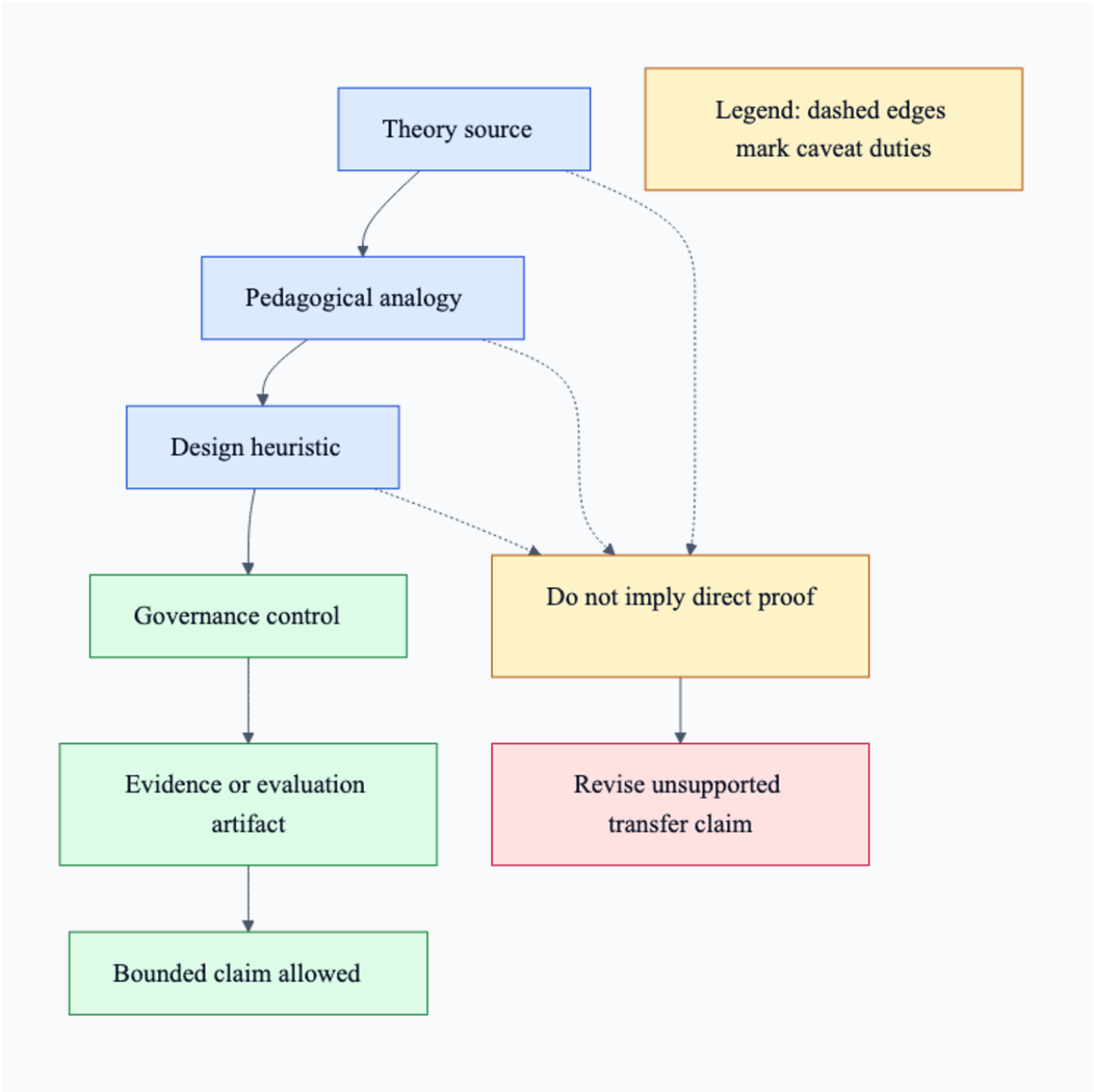


Figure 105: Conceptual schematic separating active-inference theory, pedagogical analogy, agent-design heuristic, governance control, and empirical evidence so the manuscript does not overclaim theory transfer. In the ageint agentic intelligence / active inference and ageint section, it lets readers compare Theory source, Pedagogical analogy, Design heuristic, and Governance control so the visual functions as a traceable course aid rather than an unscoped assertion.

49.2 Active-Inference Boundary Lens path for Active Inference and AGEINT: lesson cluster, safe artifact, and review

Evidence anchor. Section 49; [247, 2026].

49.2.1 Active Inference and AGEINT practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 49; [247, 2026].

49.2.2 Active Inference and AGEINT topic lessons: source-backed concepts and transfer tasks

This module builds agentic AI as delegated action under control: identity, authority, tool permissions, memory, logs, stop conditions, and recoverability define what an agent may do. The sequence opens with **The Free Energy Principle and Predictive Processing**, **Active Inference as Computational Model of Intelligence Agent Behavior**, **Shared Protentions in Multi-Agent Active Inference** and applies the **Active-Inference Boundary Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 85; module overview Section 49; curriculum atlas Section 2.

Triangulation anchors. In module 35's topic-lessons section, directly verified anchors for the **Active-Inference Theory and Governed Agent Analogy** lane include [Friston, 2010]; [Christopher L. Buckley and Seth, 2017]; [Friston, 2017]; [Da Costa, 2020]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

49.2.2.1 Lesson 1: The Free Energy Principle and Predictive Processing

Concept. The Free Energy Principle and Predictive Processing treats the free-energy principle as computational-neuroscience theory, define prediction error, generative model, and uncertainty in plain language, then show how the theory helps an analyst notice when a model is explaining too much from too little evidence.

Why it matters. The Free Energy Principle matters in the **Active-Inference Theory and Governed Agent Analogy** lane because least-privilege agent design and run evidence must stay separate from judgment; treating a formal theory as product evidence is a common failure.

Source support. The Free Energy Principle and Predictive Processing rests on [106, 2026]. The lead source's own note reads: It explains active inference as a theory describing behavior that minimizes surprise, and surveys model variants such as deep active inference, multimodal deep belief networks, predictive coding, and probabilistic programming. Use it for the working definition that **The Free Energy Principle and Predictive Processing** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Friston, 2010]; [Christopher L. Buckley and Seth, 2017].

Evidence to inspect. For **The Free Energy Principle**, work from the cited evidence behind this row. [106, 2026] A 2024 bachelor's thesis by Lara Sakarya at Delft University of Technology presenting a systematic literature review of the active inference framework and the free-energy principle as applied to mimicking social human behavior in intelligent agents. It explains active inference as a theory describing behavior that minimizes surprise, and surveys model variants such as deep active inference, multimodal deep belief networks, predictive coding, and probabilistic programming. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **The Free Energy Principle**, build a prediction-error concept card linking formal source, surprise, model assumption, analogy limit, and reviewer checkpoint. Shape **The Free Energy Principle** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that The Free Energy Principle and Predictive Processing replaces human review whenever evidence looks plausible.

Transfer task. For **The Free Energy Principle**, transfer the idea to a non-AI chapter by naming the assumed model, the surprising observation, and the review point before any decision follows.

Free-energy bound. Variational free energy F upper-bounds surprise $-\ln p(o)$ for observations o and hidden states s under a recognition density $q(s)$:

$$F = D_{\mathrm{KL}}(q(s) \,\|\, p(s \mid o)) - \ln p(o) \;\geq\; -\ln p(o).$$

Because the Kullback-Leibler term is non-negative, minimizing F over $q(s)$ tightens the bound on surprise – the precise statement of this lesson's plain-language warning about a model explaining too much from too little evidence [Friston, 2010]; [Christopher L. Buckley and Seth, 2017].

49.2.2.2 Lesson 2: Active Inference as Computational Model of Intelligence Agent Behavior

Concept. Active Inference as Computational Model of Intelligence Agent Behavior treats active inference as an agent-modeling vocabulary: beliefs, actions, expected observations, and policy selection are classroom concepts, not proof that an intelligence agent should act autonomously.

Why it matters. Analysts use **Active Inference** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that treating a formal theory as product evidence would otherwise hide, and the reviewer accountable for challenge.

Source support. Active Inference as Computational Model of Intelligence Agent Behavior rests on [003, 2026]. The lead source's own note reads: A 2021 peer-reviewed article by Stephen Fox in the journal Entropy that relates the active inference framework to social organization. Use it for the working definition that **Active Inference as Computational Model of Intelligence Agent Behavior** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Friston, 2010]; [Christopher L. Buckley and Seth, 2017].

Evidence to inspect. For **Active Inference**, reason from the sources cited in this row. [003, 2026] A 2021 peer-reviewed article by Stephen Fox in the journal Entropy that relates the active inference framework to social organization. It maps concepts such as variational free energy, prediction error, generative models, and Markov blankets onto industrial engineering and quality management practices, treating organizational survival as the maintenance of process control limits. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Active Inference**, build a toy agent-model card with beliefs, actions, observations, implementation assumption, and a human approval gate. Shape **Active Inference** work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that Active Inference as Computational Model of Intelligence Agent Behavior can be used while ignoring the rule to separate agent assistance from autonomous external action.

Transfer task. For **Active Inference**, transfer the idea to a non-AI chapter by naming the assumed model, the surprising observation, and the review point before any decision follows.

49.2.2.3 Lesson 3: Shared Protentions in Multi-Agent Active Inference

Concept. Shared Protentions in Multi-Agent Active Inference treats active inference as an agent-modeling vocabulary: beliefs, actions, expected observations, and policy selection are classroom concepts, not proof that an intelligence agent should act autonomously.

Why it matters. Shared Protentions matters in the **Active-Inference Theory and Governed Agent Analogy** lane because least-privilege agent design and run evidence must stay separate from judgment; treating a formal theory as product evidence is a common failure.

Source support. Shared Protentions in Multi-Agent Active Inference rests on [163, 2026]. The closest source to this row notes: It explains how intelligent agents can develop shared, mutually aligned expectations about future states that enable coordinated group behavior without explicit communication, drawing on Husserl's work on temporal consciousness. Use it for the claim that **Shared Protentions in Multi-Agent Active**

Inference lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Friston, 2010]; [Christopher L. Buckley and Seth, 2017].

Evidence to inspect. Ground **Shared Protentions** in the evidence the row cites. [163, 2026] An article on deniseholt.us covering a 2024 paper by VERSES AI researchers, led by Mahault Albarracin and co-authored by Karl Friston, titled Shared Protentions in Multi-Agent Active Inference. It explains how intelligent agents can develop shared, mutually aligned expectations about future states that enable coordinated group behavior without explicit communication, drawing on Husserl's work on temporal consciousness. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Shared Protentions**, build a shared-expectation register showing aligned expectations, dissent, and review ownership. Shape **Shared Protentions** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that Shared Protentions in Multi-Agent Active Inference is optional whenever separate agent assistance from autonomous external action feels inconvenient.

Transfer task. For **Shared Protentions**, transfer the idea to a non-AI chapter by naming the assumed model, the surprising observation, and the review point before any decision follows.

49.2.2.4 Lesson 4: Active Inference for Social Organization and Intelligence Communities

Concept. Active Inference for Social Organization and Intelligence Communities treats active inference as an agent-modeling vocabulary: beliefs, actions, expected observations, and policy selection are classroom concepts, not proof that an intelligence agent should act autonomously.

Why it matters. Active Inference connects classroom vocabulary to Active-Inference Theory and Governed Agent Analogy practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Active Inference for Social Organization and Intelligence Communities rests on [003, 2026]. Its anchor reference records: A 2021 peer-reviewed article by Stephen Fox in the journal Entropy that relates the active inference framework to social organization. Use it for fixing what **Active Inference for Social Organization and Intelligence Communities** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Friston, 2010]; [Christopher L. Buckley and Seth, 2017].

Evidence to inspect. For **Active Inference**, reason from the sources cited in this row. [003, 2026] A 2021 peer-reviewed article by Stephen Fox in the journal Entropy that relates the active inference framework to social organization. It maps concepts such as variational free energy, prediction error, generative models, and Markov blankets onto industrial engineering and quality management practices, treating organizational survival as the maintenance of process control limits. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Active Inference**, build an institutional feedback-loop map with incentives, review points, and oversight hooks. Shape **Active Inference** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that Active Inference for Social Organization and Intelligence Communities establishes intent without reviewing alternative explanations.

Transfer task. For **Active Inference**, transfer the idea to a non-AI chapter by naming the assumed model, the surprising observation, and the review point before any decision follows.

49.2.2.5 Lesson 5: VERSES AI Research: Multi-Scale Active Inference Architectures

Concept. VERSES AI Research: Multi-Scale Active Inference Architectures treats active inference as an agent-modeling vocabulary: beliefs, actions, expected observations, and policy selection are classroom concepts, not proof that an intelligence agent should act autonomously.

Why it matters. VERSES AI Research matters in the **Active-Inference Theory and Governed Agent Analogy** lane because least-privilege agent design and run evidence must stay separate from judgment; treating a formal theory as product evidence is a common failure.

Source support. VERSES AI Research: Multi-Scale Active Inference Architectures rests on [163, 2026] and [164, 2026]. Its anchor reference records: An article on deniseholt.us covering a 2024 paper by VERSES AI researchers, led by Mahault Albarracin and co-authored by Karl Friston, titled Shared Protentions in Multi-Agent Active Inference. Use them for the working definition that **VERSES AI Research: Multi-Scale Active Inference Architectures** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Friston, 2010]; [Christopher L. Buckley and Seth, 2017].

Evidence to inspect. For **VERSES AI Research**, reason from the sources cited in this row. [163, 2026] An article on deniseholt.us covering a 2024 paper by VERSES AI researchers, led by Mahault Albarracin and co-authored by Karl Friston, titled Shared Protentions in Multi-Agent Active Inference. It explains how intelligent agents can develop shared, mutually aligned expectations about future states that enable coordinated group behavior without explicit communication, drawing on Husserl's work on temporal consciousness. [164, 2026] A press release from VERSES AI (August 2024) announcing that the company would act as lead sponsor of and present research at the 5th International Workshop on Active Inference (IWAI 2024) in Oxford. It states that VERSES researchers had 12 accepted papers spanning foundational capabilities, multi-agent systems, applications, and ethics, and that the company's chief scientist Karl Friston would speak. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **VERSES AI Research**, build an architecture-claim card separating research claims, implementation assumptions, and governance limits. Shape **VERSES AI Research** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that VERSES AI Research: Multi-Scale Active Inference Architectures replaces human review whenever evidence looks plausible.

Transfer task. For **VERSES AI Research**, transfer the idea to a non-AI chapter by naming the assumed model, the surprising observation, and the review point before any decision follows.

49.2.2.6 Lesson 6: Cognitive Security Through the Active Inference Lens

Concept. Cognitive Security Through the Active Inference Lens treats active inference as an agent-modeling vocabulary: beliefs, actions, expected observations, and policy selection are classroom concepts, not proof that an intelligence agent should act autonomously.

Why it matters. Analysts use **Cognitive Security** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that treating a formal theory as product evidence would otherwise hide, and the reviewer accountable for challenge.

Source support. Cognitive Security Through the Active Inference Lens rests on [105, 2026]. The lead source's own note reads: Sarah Rajtmajer and Daniel Susser, 'Automated Influence and the Challenge of Cognitive Security,' in Hot Topics in the Science of Security (HotSoS '20), April 2020, ACM. Use it for pinning down the scope of **Cognitive Security Through the Active Inference Lens**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Friston, 2010]; [Christopher L. Buckley and Seth, 2017].

Evidence to inspect. For **Cognitive Security**, work from the cited evidence behind this row. [105, 2026] Sarah Rajtmajer and Daniel Susser, 'Automated Influence and the Challenge of Cognitive Security,' in Hot Topics in the Science of Security (HotSoS '20), April 2020, ACM. The paper argues that AI-powered computational propaganda poses national security threats that existing ethical frameworks do not address, and proposes 'cognitive security' as a productive conceptual lens for evaluating the ethics of automated influence operations and potential defensive responses. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Cognitive Security**, build a sample narrative-risk map with provenance, audience harm, and transparent response options. Shape **Cognitive Security** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that Cognitive Security Through the Active Inference Lens can be used while ignoring the rule to separate agent assistance from autonomous external action.

Transfer task. For **Cognitive Security**, transfer the idea to a non-AI chapter by naming the assumed model, the surprising observation, and the review point before any decision follows.

49.2.2.7 Lesson 7: Applications: Deception Detection, Surprise Minimization, Threat Modeling

Concept. Applications: Deception Detection, Surprise Minimization, Threat Modeling compares deception indicators with alternative explanations and uncertainty before any operational inference.

Why it matters. Applications: Deception Detection, Surprise Minimization, Threat Modeling matters in the **Active-Inference Theory and Governed Agent Analogy** lane because least-privilege agent design and run evidence must stay separate from judgment; treating a formal theory as product evidence is a common failure.

Source support. Applications: Deception Detection, Surprise Minimization, Threat Modeling rests on [309, 2026], [310, 2026], and [300, 2026]. The closest source to this row notes: It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). Use them for fixing what **Applications: Deception Detection, Surprise Minimization, Threat Modeling** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Friston, 2010]; [Christopher L. Buckley and Seth, 2017].

Evidence to inspect. Ground **Applications: Deception Detection, Surprise Minimization, Threat Modeling** in the evidence the row cites. [309, 2026] An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection. [310, 2026] The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Applications**, build a threat-model review card with assumptions, disconfirming evidence, and confidence language. Shape **Applications: Deception Detection, Surprise Minimization, Threat Modeling** work as an **agent run and assurance card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that Applications: Deception Detection, Surprise Minimization, Threat Modeling is optional whenever separate agent assistance from autonomous external action feels inconvenient.

Transfer task. Transfer **Applications: Deception Detection, Surprise Minimization, Threat Modeling** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

49.2.2.8 Lesson 8: Applications of Active Inference and FEP in Intelligence (TU Delft Thesis)

Concept. Applications of Active Inference and FEP in Intelligence (TU Delft Thesis) treats active inference as an agent-modeling vocabulary: beliefs, actions, expected observations, and policy selection are classroom concepts, not proof that an intelligence agent should act autonomously.

Why it matters. Analysts use **Applications of Active Inference and FEP in Intelligence (TU Delft Thesis)** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that treating a formal theory as product evidence would otherwise hide, and the reviewer accountable for challenge.

Source support. Applications of Active Inference and FEP in Intelligence (TU Delft Thesis) rests on [106, 2026]. The most specific cited work observes: It explains active inference as a theory describing behavior that minimizes surprise, and surveys model variants such as deep active inference, multimodal deep belief networks, predictive coding, and probabilistic programming. Use it for the claim that **Applications of Active Inference and FEP in Intelligence (TU Delft Thesis)** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Friston, 2010]; [Christopher L. Buckley and Seth, 2017].

Evidence to inspect. Read **Applications of Active Inference and FEP in Intelligence (TU Delft Thesis)** against the works cited for this row. [106, 2026] A 2024 bachelor's thesis by Lara Sakarya at Delft University of Technology presenting a systematic literature review of the active inference framework and the free-energy principle as applied to mimicking social human behavior in intelligent agents. It explains active inference as a theory describing behavior that minimizes surprise, and surveys model variants such as deep active inference, multimodal deep belief networks, predictive coding, and probabilistic programming. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Applications of Active Inference and FEP in Intelligence (TU Delft Thesis)**, build a research question, method, evidence base, and classroom boundary statement for the thesis topic. Shape this subject work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that Applications of Active Inference and FEP in Intelligence (TU Delft Thesis) establishes intent without reviewing alternative explanations.

Transfer task. For **Applications of Active Inference and FEP in Intelligence (TU Delft Thesis)**, transfer the idea to a non-AI chapter by naming the assumed model, the surprising observation, and the review point before any decision follows.

49.2.3 Active Inference and AGEINT worked safe example: synthetic inputs, evidence, and review

Worked example: a synthetic research assistant agent organizes public readings for an instructor. [247, 2026]; [248, 2026].

Triangulation anchors. In module 35's worked-example section, directly verified anchors for the **Active-Inference Theory and Governed Agent Analogy** lane include [Friston, 2010]; [Christopher L. Buckley and Seth, 2017]; [Friston, 2017]; [Da Costa, 2020]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **governed agentic intelligence**. Learners use a **agent run and assurance card** and keep this boundary visible: No autonomous external action, credentialed operations, live-target workflows, or uncontrolled tool use.

Frame. The classroom question centers on **The Free Energy Principle and Predictive Processing**. Excluded actions stay explicit, and the **Active-Inference Boundary Lens** planning question is: Which layer is formal theory, which layer is classroom analogy, which implementation claim needs evidence, and which governance control prevents autonomy overreach?

Inputs. For the **The Free Energy Principle and Predictive Processing** scenario, use public URLs, a fixed retrieval tool, a summarization prompt, a time budget, and a stop condition. The Active-Inference Boundary Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **The Free Energy Principle and Predictive Processing**, students bind the agent identity, list allowed tools, set autonomy limits, capture sources, block unsafe requests, and log approvals. Pause whenever an inference about The Free Energy Principle and Predictive Processing appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **The Free Energy Principle and Predictive Processing** classroom scenario; unit artifact = agent run and assurance card; evidence = allowed inputs; method = least-privilege agent design and run review; output = an agent run card with tool calls, source links, blocked actions, reviewer notes, incident threshold, and recovery decision; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **The Free Energy Principle and Predictive Processing** as "Active-Inference Boundary Lens confirms it" is not enough. The revision ties the claim to least-privilege agent design and run review, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **The Free Energy Principle and Predictive Processing** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

49.2.4 Active Inference and AGEINT practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Active-Inference Boundary Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**.

Triangulation anchors. In module 35's practice-sequence section, directly verified anchors for the **Active-Inference Theory and Governed Agent Analogy** lane include [Friston, 2010]; [Christopher L. Buckley and Seth, 2017]; [Friston, 2017]; [Da Costa, 2020]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare The Free Energy Principle and Predictive Processing, Active Inference as Computational Model of Intelligence Agent Behavior, Shared Protentions in Multi-Agent Active Inference; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Active-Inference Theory and Governed Agent Analogy** lane.
2. Frame	Answer the lens question: Which layer is formal theory, which layer is classroom analogy, which implementation claim needs evidence, and which governance control prevents autonomy overreach?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for The Free Energy Principle and Predictive Processing: theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the agent run and assurance card fields for The Free Energy Principle and Predictive Processing.	Unit profile note.	Evidence artifacts include tool-allowlist record, external-memory governance boundary.
4. Challenge	Test the misconception that The Free Energy Principle and Predictive Processing replaces human review whenever evidence looks plausible.	Failure-mode note.	The artifact applies the key distinction: separate agent assistance from autonomous external action.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

49.2.4.1 Active Inference and AGEINT instructor notes: source reasoning, review points, and studio focus

Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**. [247, 2026]; [248, 2026].

49.2.4.2 Active Inference and AGEINT extension exercise: peer validation and refresh trigger review

Evidence anchor. Section 49; [247, 2026].

Have learners swap artifacts and apply the **Active-Inference Boundary Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**.

49.2.5 Active Inference and AGEINT knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 49; [247, 2026].

1. Explain how **The Free Energy Principle and Predictive Processing** is defined here; name the source descriptor that supports the definition.
2. Contrast **The Free Energy Principle and Predictive Processing** with **Active Inference as Computational Model of Intelligence Agent Behavior** using the **Active-Inference Boundary Lens** artifact fields.
3. Identify one failure mode from the **Active-Inference Theory and Governed Agent Analogy** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which permission can be removed while preserving the learning objective?
5. Correct this misconception: that The Free Energy Principle and Predictive Processing replaces human review whenever evidence looks plausible.

49.2.5.1 Active Inference and AGEINT answer quality rubric: source evidence, uncertainty, and safe transfer

Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **The Free Energy Principle and Predictive Processing** without source evidence, uncertainty, or a safe transfer task.

49.3 Active Inference and AGEINT assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 49; [247, 2026].

49.3.1 Active Inference and AGEINT evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 49; [247, 2026].

49.3.2 Active Inference and AGEINT transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 49; [247, 2026].

49.3.2.1 Active Inference and AGEINT lineage and source tradition: profile, concepts, and first anchors This sits in the **Active-Inference Theory and Governed Agent Analogy** lineage: using free-energy and active-inference theory as a bounded computational vocabulary for perception, action, uncertainty, and policy selection while keeping AGEINT governance claims separate. [247, 2026]; [248, 2026].

49.3.2.2 Active Inference and AGEINT working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 49; [247, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**, with provenance and reviewability throughout.

49.3.2.3 Active Inference and AGEINT knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [247, 2026]; [248, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

49.3.2.4 Active Inference and AGEINT transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 49; [247, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**.
- **Evidence contract:** keep the **Active-Inference Theory and Governed Agent Analogy** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

49.3.2.5 Active Inference and AGEINT profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 49; [247, 2026].

The matched profile emphasizes using free-energy and active-inference theory as a bounded computational vocabulary for perception, action, uncertainty, and policy selection while keeping AGEINT governance claims separate. The method stack is formal-source review, theory-to-analogy mapping, assumption listing, implementation-evidence check, governance-control mapping, and human-review caveat; the local topic cluster is **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**.

49.3.3 Active Inference and AGEINT evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 49; [247, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Active-Inference Theory and Governed Agent Analogy** profile tells reviewers what evidence is strong enough for the module artifact built around **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**.

49.3.3.1 Active Inference and AGEINT guide source spine: inherited keys and local citation roles Primary guide citations: [247, 2026]; [248, 2026]; [265, 2026]; [278, 2026]; [279, 2026]; [283, 2026]; [290, 2026]; [291, 2026]; [294, 2026]; [106, 2026]; [003, 2026]; [163, 2026]; [164, 2026]; [105, 2026]; [299, 2026]; [306, 2026]; [312, 2026]; [309, 2026]; [310, 2026]; [300, 2026].

49.3.3.2 Active Inference and AGEINT verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [247, 2026]; [248, 2026].

Tier	What counts	How it is used
Source guide	[247, 2026]; [248, 2026]; [265, 2026]; [278, 2026]; [279, 2026]; [283, 2026]; [290, 2026]; [291, 2026]; [294, 2026]; [106, 2026]; [003, 2026]; [163, 2026]; [164, 2026]; [105, 2026]; [299, 2026]; [306, 2026]; [312, 2026]; [309, 2026]; [310, 2026]; [300, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 35's source-canon section, directly verified anchors for the **Active-Inference Theory and Governed Agent Analogy** lane include [Friston, 2010]; [Christopher L. Buckley and Seth, 2017]; [Friston, 2017]; [Da Costa, 2020]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior** and [247, 2026]; [248, 2026], but only directly verified source URLs are encoded as citations.

49.3.3.3 Active Inference and AGEINT intelligence practice lens: evidence artifact and safety check Practice lens: **Active-Inference Boundary Lens** for **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**. [247, 2026]; [248, 2026].

Planning question: Which layer is formal theory, which layer is classroom analogy, which implementation claim needs evidence, and which governance control prevents autonomy overreach?

Evidence artifact: theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition.

Validation rule: separate formal claim, pedagogical analogy, implementation assumption, evaluation evidence, and governance duty before reuse. Applied to **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**.

Handoff contract: handoff preserves formal source, analogy scope, source limitation, caveat, reviewer owner, and blocked autonomous-action claim.

Safety check: reject claims that the free-energy principle proves autonomous agency, intent, detection performance, or oversight-free action.

49.3.3.4 Active Inference and AGEINT runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 49; [247, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	35.99	35.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Active Inference and AGEINT to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
AGEINT pattern registry, agent identity, and interface-contract studio	35.100	35.100 source title transformed into safe curriculum treatment; original: V2 AGEINT-depth extension: connect active-inference planning to public-sector service adoption, workforce impact, skills governance, and human-centered oversight rather than autonomous agency	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Bounded autonomy, procurement, incident-response, and assurance studio	35.101	35.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Active Inference and AGEINT	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Model-card, recoverability, retention, and learner-support evidence package	35.102	35.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Active Inference and AGEINT	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
The Free Energy Principle and Predictive Processing	35.1	35.1 The Free Energy Principle and Predictive Processing	Active-Inference Boundary Lens	theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition	reject claims that the free-energy principle proves autonomous agency, intent, detection performance, or oversight-free action
Active Inference as Computational Model of Intelligence Agent Behavior	35.2	35.2 Active Inference as Computational Model of Intelligence Agent Behavior	Active-Inference Boundary Lens	theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition	reject claims that the free-energy principle proves autonomous agency, intent, detection performance, or oversight-free action
Shared Protentions in Multi-Agent Active Inference	35.3	35.3 Shared Protentions in Multi-Agent Active Inference	Active-Inference Boundary Lens	theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition	reject claims that the free-energy principle proves autonomous agency, intent, detection performance, or oversight-free action
Active Inference for Social Organization and Intelligence Communities	35.4	35.4 Active Inference for Social Organization and Intelligence Communities	Active-Inference Boundary Lens	theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition	reject claims that the free-energy principle proves autonomous agency, intent, detection performance, or oversight-free action
VERSES AI Research: Multi-Scale Active Inference Architectures	35.5	35.5 VERSES AI Research: Multi-Scale Active Inference Architectures	Active-Inference Boundary Lens	theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition	reject claims that the free-energy principle proves autonomous agency, intent, detection performance, or oversight-free action
Cognitive Security Through the Active Inference Lens	35.6	35.6 Cognitive Security Through the Active Inference Lens	Active-Inference Boundary Lens	theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition	reject claims that the free-energy principle proves autonomous agency, intent, detection performance, or oversight-free action
Applications: Deception Detection, Surprise Minimization, Threat Modeling	35.7	35.7 Applications: Deception Detection, Surprise Minimization, Threat Modeling	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Applications of Active Inference and FEP in Intelligence (TU Delft Thesis)	35.8	35.8 Applications of Active Inference and FEP in Intelligence (TU Delft Thesis)	Active-Inference Boundary Lens	theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition	reject claims that the free-energy principle proves autonomous agency, intent, detection performance, or oversight-free action

49.3.3.5 Active Inference and AGEINT reusable subsection contract: topic rows, artifacts, and safety duties **Evidence anchor.** Section 49; [247, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
The Free Energy Principle and Predictive Processing	Active-Inference Boundary Lens	theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition	reject claims that the free-energy principle proves autonomous agency, intent, detection performance, or oversight-free action
Active Inference as Computational Model of Intelligence Agent Behavior	Active-Inference Boundary Lens	theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition	reject claims that the free-energy principle proves autonomous agency, intent, detection performance, or oversight-free action
Shared Protentions in Multi-Agent Active Inference	Active-Inference Boundary Lens	theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition	reject claims that the free-energy principle proves autonomous agency, intent, detection performance, or oversight-free action
Active Inference for Social Organization and Intelligence Communities	Active-Inference Boundary Lens	theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition	reject claims that the free-energy principle proves autonomous agency, intent, detection performance, or oversight-free action
VERSES AI Research: Multi-Scale Active Inference Architectures	Active-Inference Boundary Lens	theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition	reject claims that the free-energy principle proves autonomous agency, intent, detection performance, or oversight-free action
Cognitive Security Through the Active Inference Lens	Active-Inference Boundary Lens	theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition	reject claims that the free-energy principle proves autonomous agency, intent, detection performance, or oversight-free action
Applications: Deception Detection, Surprise Minimization, Threat Modeling	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Applications of Active Inference and FEP in Intelligence (TU Delft Thesis)	Active-Inference Boundary Lens	theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition	reject claims that the free-energy principle proves autonomous agency, intent, detection performance, or oversight-free action

49.3.3.6 Active Inference and AGEINT annotated source ledger: real titles and local contribution Each source cited by this **Active-Inference Theory and Governed Agent Analogy** module is paired below with its real title and a one-line note on what it contributes to **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**.

Source	Cited work	What it contributes	Status
[247, 2026]	AI in the Public Sector	Official OECD.AI public-sector AI theme page.	original source-guide
[248, 2026]	Artificial Intelligence Working Group	The World Bank GovTech program page for its Artificial Intelligence Working Group, a community of government technology experts focused on knowledge-sharing and policy tools for responsible public-sector AI adoption. It notes that many developing countries face barriers such as limited digital skills, infrastructure, and data, which risk widening global inequality.	verified source-guide
[265, 2026]	AI and Work	Official OECD.AI work theme page.	original source-guide
[278, 2026]	Recommendation of the Council on Public Procurement	The OECD Recommendation of the Council on Public Procurement (OECD/LEGAL/0411), a legal instrument adopted by the OECD Council in 2015 on the proposal of the Public Governance Committee. It frames public procurement as a pillar of strategic governance and service delivery and sets out principles for governments to follow.	verified source-guide

Source	Cited work	What it contributes	Status
[279, 2026]	Open Contracting Data Standard	The documentation homepage for the Open Contracting Data Standard, version 1.1.5, maintained by the Open Contracting Partnership to support disclosure of government contracting data across the procurement lifecycle. It provides a common data model spanning planning, tender, award, contract, and implementation stages, along with a primer, implementation guidance, technical schemas, and validation tooling.	verified source-guide
[283, 2026]	Recommendation of the Council on Open Government	An OECD legal instrument document reproducing the Recommendation of the Council on Open Government (OECD/LEGAL/0438), adopted on 14 December 2017. It defines open government as a culture of governance promoting transparency, integrity, accountability, and stakeholder participation in support of democracy and inclusive growth.	verified source-guide
[290, 2026]	NIST SP 800-218A: Secure Software Development Practices for Generative AI and Dual-Use Foundation Models	NIST Special Publication 800-218A (July 2024), which augments the Secure Software Development Framework with practices specific to AI model development across the software lifecycle. Produced in response to Executive Order 14110, it addresses AI model producers, developers building on those models, and acquirers of AI systems, and is designed to be used alongside NIST SP 800-218.	verified source-guide
[291, 2026]	Revised 508 Standards and 255 Guidelines	Official documentation from the U.S. Access Board on the Revised 508 Standards and 255 Guidelines for information and communication technology accessibility. It establishes mandatory accessibility requirements for federal agencies and voluntary guidelines for telecommunications manufacturers, covering hardware, software, websites, electronic documents, and support services.	verified source-guide
[294, 2026]	M-25-21: Accelerating Federal Use of AI through Innovation, Governance, and Public Trust	An April 2025 Office of Management and Budget memorandum (M-25-21) directing executive branch agencies on federal use of artificial intelligence. Issued under Executive Order 14179, it instructs agencies to accelerate adoption of AI to improve public services and government efficiency while maintaining safeguards for civil rights, civil liberties, and privacy.	verified source-guide
[106, 2026]	Applications of The Active Inference and The Free-Energy Principle	A 2024 bachelor's thesis by Lara Sakarya at Delft University of Technology presenting a systematic literature review of the active inference framework and the free-energy principle as applied to mimicking social human behavior in intelligent agents. It explains active inference as a theory describing behavior that minimizes surprise, and surveys model variants such as deep active inference, multimodal deep belief networks, predictive coding, and probabilistic programming.	verified source-guide

Source	Cited work	What it contributes	Status
[003, 2026]	Active Inference: Applicability to Different Types of Social	A 2021 peer-reviewed article by Stephen Fox in the journal Entropy that relates the active inference framework to social organization. It maps concepts such as variational free energy, prediction error, generative models, and Markov blankets onto industrial engineering and quality management practices, treating organizational survival as the maintenance of process control limits.	verified source-guide
[163, 2026]	Karl Friston's Groundbreaking Research Lays the Foundation	An article on deniseholt.us covering a 2024 paper by VERSES AI researchers, led by Mahault Albarracin and co-authored by Karl Friston, titled Shared Protentions in Multi-Agent Active Inference. It explains how intelligent agents can develop shared, mutually aligned expectations about future states that enable coordinated group behavior without explicit communication, drawing on Husserl's work on temporal consciousness.	verified source-guide
[164, 2026]	VERSES to Present Research at Active Inference Workshop	A press release from VERSES AI (August 2024) announcing that the company would act as lead sponsor of and present research at the 5th International Workshop on Active Inference (IWAI 2024) in Oxford. It states that VERSES researchers had 12 accepted papers spanning foundational capabilities, multi-agent systems, applications, and ethics, and that the company's chief scientist Karl Friston would speak.	verified source-guide
[105, 2026]	Automated influence and the challenge of cognitive security	Sarah Rajtmajer and Daniel Susser, 'Automated Influence and the Challenge of Cognitive Security,' in Hot Topics in the Science of Security (HotSoS '20), April 2020, ACM. The paper argues that AI-powered computational propaganda poses national security threats that existing ethical frameworks do not address, and proposes 'cognitive security' as a productive conceptual lens for evaluating the ethics of automated influence operations and potential defensive responses.	verified source-guide
[299, 2026]	Model Context Protocol Specification	The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation).	verified source-guide context; use pinned MCP anchor for normative claims
[306, 2026]	Artificial Intelligence	Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support.	original source-guide
[312, 2026]	Guide on the Use of Agentic Artificial Intelligence	Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support.	original source-guide

Source	Cited work	What it contributes	Status
[309, 2026]	STIX Version 2.1	An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection.	verified source-guide
[310, 2026]	TAXII Version 2.1	The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe).	verified source-guide
[300, 2026]	MITRE ATLAS	MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy.	original source-guide

Where this sits. This module's overview is Section 49; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

49.3.4 Active Inference and AGEINT governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 49; [247, 2026].

49.3.5 Active Inference and AGEINT analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 35's governance-boundary section, directly verified anchors for the **Active-Inference Theory and Governed Agent Analogy** lane include [Friston, 2010]; [Christopher L. Buckley and Seth, 2017]; [Friston, 2017]; [Da Costa, 2020]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Research lane: **Agentic AI Governance and Tool Security** for **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**. [247, 2026]; [248, 2026].
Curriculum topic spine: The Free Energy Principle and Predictive Processing, **Active Inference as Computational Model of Intelligence Agent Behavior**, **Shared Protentions in Multi-Agent Active Inference**. **Verified anchor cluster:** [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]; [Community, 2020b]; [Community, 2020a]; [of the Director of National Intelligence, 2025b].
Conceptual depth: delegated action under explicit authority, identity, permissions, tool boundaries, monitoring, and human escalation.
Method stack: AI RMF Govern-Map-Measure-Manage, least-privilege tool design, prompt-injection review, progressive deployment, and rollback drills.
Composability contract: agents, tools, credentials, memory, retrieval stores, policies, and logs remain separately inspectable and revocable components.
Known failure modes: excessive agency, shadow tools, indirect prompt injection, memory poisoning, confused authority, and unbounded action chains.
Defensive boundary: agentic workflows stay synthetic, owned-lab, supervised, logged, rate-limited, and reversible unless a lawful production authority exists. Applied to **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**.

Anchor	Why it matters here
[OECD, 2026a]	Official OECD conceptual foundation for agentic AI. Checked as of 2026-05-21; role: source_quality_anchor.
[of Canada Secretariat, 2026a]	Government of Canada guide for accountable public-sector use of agentic AI, including governance, risk, transparency, testing, monitoring, and human oversight considerations. Checked as of 2026-05-24; role: curriculum_anchor.
[of Standards and Technology, 2023]	Official NIST.AI.100-1 risk-management framework. Checked as of 2026-05-21; role: source_quality_anchor.
[of Standards and Technology, 2024d]	Official NIST AI 600-1 generative AI profile. Checked as of 2026-05-21; role: source_quality_anchor.
[Community, 2020b]	Official IC principles for lawful, accountable, objective, human-centered, secure, resilient, and science-informed AI. Checked as of 2026-05-21; role: curriculum_anchor.
[Community, 2020a]	Official IC framework for AI goals, authorities, human judgment, bias mitigation, testing, documentation, explainability, and review. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2025b]	Official IC AI governance directive covering CAIO roles, oversight, interoperability, civil-liberties review, training data, and impact assessment. Checked as of 2026-05-21; role: curriculum_anchor.

49.3.5.1 Active Inference and AGEINT evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **Active-Inference Theory and Governed Agent Analogy** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [247, 2026]; [248, 2026].

49.3.6 Active Inference and AGEINT agentic boundary: assist, approve, block, and record

Evidence anchor. Section 49; [247, 2026].
AGEINT translation is bounded by the **Active-Inference Theory and Governed Agent Analogy** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**.

49.3.6.1 Active Inference and AGEINT permitted defensive utility: curriculum uses and safe outputs

Evidence anchor. Section 49; [247, 2026].
The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**.

49.3.6.2 Active Inference and AGEINT excluded operational boundary: blocked actions and stop rules

Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [247, 2026]; [248, 2026] and **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

49.3.7 Active Inference and AGEINT governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 49; [247, 2026].
Governance is practiced as a gate on the **Active-Inference Theory and Governed Agent Analogy** lane. Learners use the **Active-Inference Boundary Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**.

49.3.7.1 Active Inference and AGEINT governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [247, 2026]; [248, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Active-Inference Theory and Governed Agent Analogy** failure modes and the **Active-Inference Boundary Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

49.3.7.2 Active Inference and AGEINT evidence package handoff: appendices, records, and reuse

Evidence anchor. Section 49; [247, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Active-Inference Boundary Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**.

49.3.7.3 Active Inference and AGEINT current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**. [247, 2026]; [248, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `scholarly_friston_2010_fep` for **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**?	The free-energy principle: a unified brain theory?; lane `cognitive_active_inference`; checked 2026-06-08.	theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition; Karl Friston's flagship review introducing the free-energy principle, showing how a variational free-energy functional provides a tractable upper bound on surprise (negative log model evidence) that the brain minimizes through perception and action.
What does the module inherit from `scholarly_buckley_2017_fep_mathematical_review` for **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**?	The Free Energy Principle for Action and Perception: A Mathematical Review; lane `cognitive_active_inference`; checked 2026-06-10.	theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition; active-inference theory review, classroom analogy boundary setting, formal-claim caveat review, and governance handoff evidence
What does the module inherit from `scholarly_friston_2017_active_inference_process` for **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**?	Active Inference: A Process Theory; lane `cognitive_active_inference`; checked 2026-06-08.	theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition; Formalizes active inference as a process theory in which belief updating proceeds by gradient descent on variational free energy and policies are selected by minimizing expected free energy over a Markov decision process generative model.
What does the module inherit from `scholarly_dacosta_2020_discrete_active_inference` for **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**?	Active inference on discrete state-spaces: A synthesis; lane `cognitive_active_inference`; checked 2026-06-08.	theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition; A mathematical synthesis of active inference over discrete (POMDP) state-spaces, consolidating the partially observable Markov decision process model used to specify perception, planning, and action selection in agentic systems.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 49; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

49.3.8 Active Inference and AGEINT assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 49; [247, 2026].

49.3.9 Active Inference and AGEINT assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 49; [247, 2026].

49.3.9.1 Active Inference and AGEINT capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior** and [247, 2026]; [248, 2026].

49.3.9.2 Active Inference and AGEINT instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior** and [247, 2026]; [248, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

49.3.9.3 Active Inference and AGEINT assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
The Free Energy Principle and Predictive Processing	Completed **theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Active Inference as Computational Model of Intelligence Agent Behavior	Completed **theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Shared Protentions in Multi-Agent Active Inference	Completed **theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

49.3.10 Active Inference and AGEINT refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [247, 2026]; [248, 2026] and **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**.

49.3.10.1 Active Inference and AGEINT refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**. The local signals begin with [247, 2026]; [248, 2026].

49.3.10.2 Active Inference and AGEINT claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**, and the source spine for these checks begins with [247, 2026]; [248, 2026].

49.3.11 Active Inference and AGEINT reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [247, 2026]; [248, 2026].

Triangulation anchors. In module 35's review-checklist section, directly verified anchors for the **Active-Inference Theory and Governed Agent Analogy** lane include [Friston, 2010]; [Christopher L. Buckley and Seth, 2017]; [Friston, 2017]; [Da Costa, 2020]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior**. [247, 2026]; [248, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

49.3.12 Active Inference and AGEINT learning-path links: module map, overview, and curriculum atlas

Use the cross-links below to place **The Free Energy Principle and Predictive Processing; Active Inference as Computational Model of Intelligence Agent Behavior** in the wider unit: the orientation sets the frame, the parent unit supplies the shared safety posture, and the neighbouring modules show what evidence enters and leaves. Lead sources: [247, 2026]; [248, 2026].

Section 2, Section 44, Section 48, Section 50

50 AGEINT Python Code Library

50.0.1 AGEINT Python Code Library figures and course links: visual evidence, source flow, and navigation

The module uses Figure 106 and Figure 85 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 44, Section 49, Section 51.
This module teaches the **Agentic AI Governance and Tool Security** lane through a bounded, source-backed coursebook chapter. [242, 2026]; [243, 2026].

50.1 Agentic AI Governance and Tool Security frame for AGEINT Python Code Library: source context, topic focus, and reader task

Evidence anchor. Section 50; [242, 2026].

50.1.1 AGEINT Python Code Library orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 50; [242, 2026].

50.1.2 AGEINT Python Code Library conceptual primer: source context, core model, and reader task

This chapter teaches agentic AI as delegated action under control: identity, authority, tool permissions, memory, logs, stop conditions, and recoverability define what an agent may do. The chapter uses **Agentic Tool-Governance Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**.
The central distinction is to separate agent assistance from autonomous external action. Core topics include **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records; Autonomous Vulnerability Scanner: AutoGen + Nmap + MITRE ATT&CK Navigator**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [242, 2026]; [243, 2026].
Learners move from vocabulary and the **Agentic Tool-Governance Lens** distinction through topic lessons on **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII** with evidence and misconception checks, then assemble an **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** with safety and rights gates.

50.1.3 AGEINT Python Code Library learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 50; [242, 2026].

- Connect **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII and Search-exposure provenance review using instructor-provided records** to **Agentic AI Governance and Tool Security** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build an **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate agent assistance from autonomous external action; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as excessive agency, shadow tools, indirect prompt injection, memory poisoning, confused authority, and unbounded action chains, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: agentic workflows stay synthetic, owned-lab, supervised, logged, rate-limited, and reversible unless a lawful production authority exists.

50.1.4 AGEINT Python Code Library core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 50; [242, 2026].

Term	Working definition
Agent identity	the named software actor, role, and authorization context for a run
Tool allowlist	the bounded set of actions the agent may request
Delegation	the handoff of a task under explicit human authority and review
Bounded autonomy	the documented ceiling on what an agent may decide or request without review
Recoverability	the path back to a known-safe state after a bad output or action request
AI incident	a logged event where an AI system creates or plausibly creates harm or loss of control
Prompt injection	untrusted content that attempts to override instructions or authority boundaries
Pattern registry	the catalog of approved agent behaviors, prompts, and evaluation hooks
Adversarial eval	structured tests that probe agent misuse, injection, and over-delegation before release
Threat Intelligence Aggregation Agent:…	Key terms: Threat, Aggregation, Agent.
Search-exposure provenance review using…	Key terms: Search, exposure, provenance.

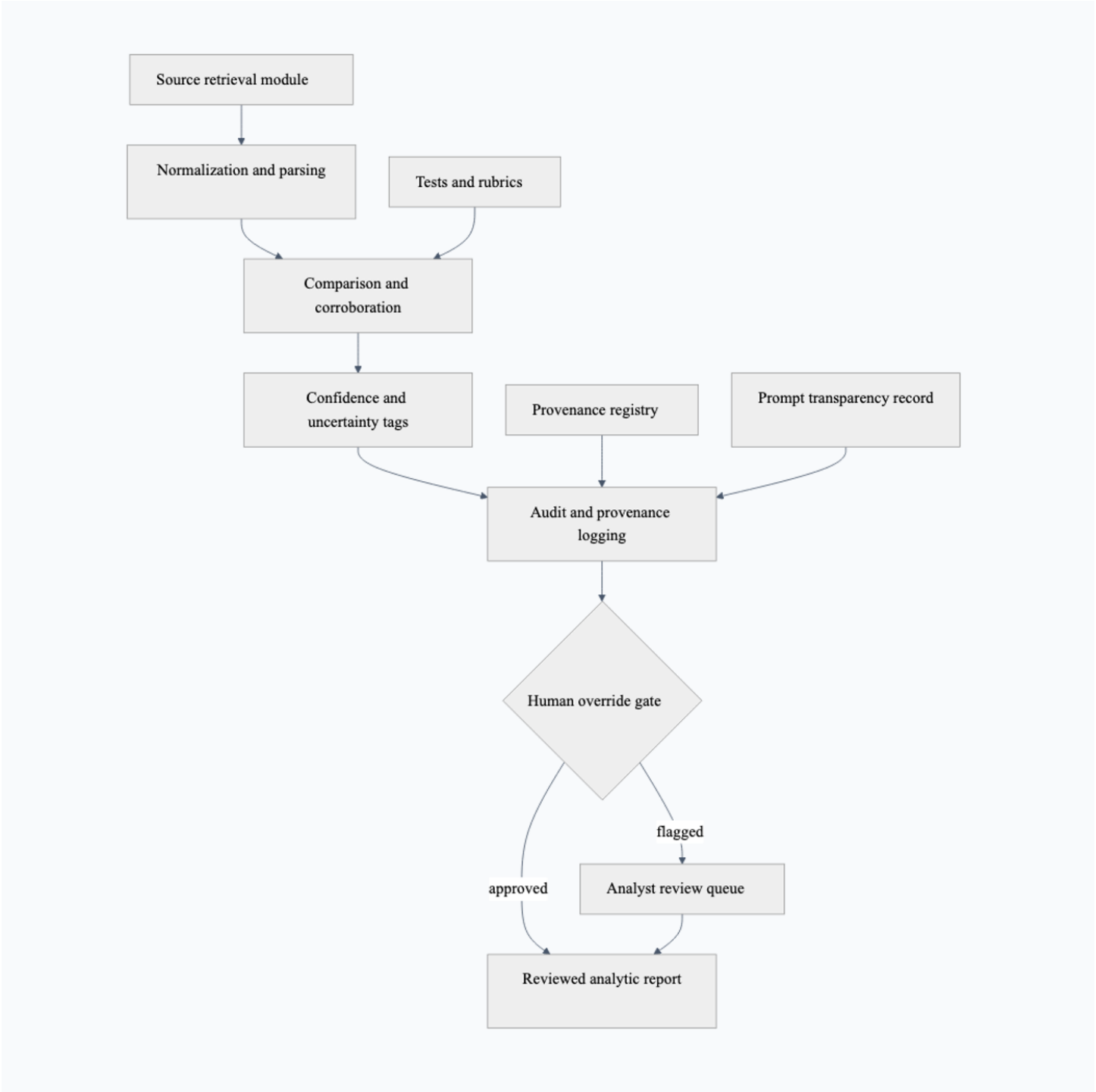


Figure 106: A module map of the library's defensive building blocks, where retrieval, comparison, and audit components always route through a human-override gate. It is anchored to the ageint agentic intelligence / ageint python code library section; use it to inspect Source retrieval module, Normalization and parsing, Comparison and corroboration, and Confidence and uncertainty tags while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

50.2 Agentic Tool-Governance Lens path for AGEINT Python Code Library: lesson cluster, safe artifact, and review

Evidence anchor. Section 50; [242, 2026].

50.2.1 AGEINT Python Code Library practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 50; [242, 2026].

50.2.2 AGEINT Python Code Library topic lessons: source-backed concepts and transfer tasks

This module builds agentic AI as delegated action under control: identity, authority, tool permissions, memory, logs, stop conditions, and recoverability define what an agent may do. The sequence opens with **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII**, **Search-exposure provenance review using instructor-provided records**, **Autonomous Vulnerability Scanner: AutoGen + Nmap + MITRE ATT&CK Navigator** and applies the **Agentic Tool-Governance Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 85; module overview Section 50; curriculum atlas Section 2.

Triangulation anchors. In module 36's topic-lessons section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

50.2.2.1 Lesson 1: Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII

Concept. Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII uses sharing standards to document indicator context, handling, confidence, and consumer responsibilities—not raw indicator hoarding.

Why it matters. Threat Intelligence Aggregation Agent matters in the **Agentic AI Governance and Tool Security** lane because least-privilege agent design and run evidence must stay separate from judgment; excessive agency is a common failure.

Source support. Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII rests on [309, 2026], [310, 2026], and [300, 2026]. The lead source's own note reads: It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). Use them for fixing what **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **Threat Intelligence Aggregation Agent** against the works cited for this row. [309, 2026] An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection. [310, 2026] The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Threat Intelligence Aggregation Agent**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the source descriptor, the bounded claim about **Threat Intelligence Aggregation Agent**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Threat Intelligence Aggregation Agent** work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII replaces human review whenever evidence looks plausible.

Transfer task. Transfer **Threat Intelligence Aggregation Agent** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

50.2.2.2 Lesson 2: Search-exposure provenance review using instructor-provided records

Concept. Search-exposure provenance review using instructor-provided records treats open sources as publicly available evidence that still requires provenance, corroboration, legality, and minimization before reuse.

Why it matters. Analysts use **Search-exposure provenance review** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that excessive agency would otherwise hide, and the reviewer accountable for challenge.

Source support. Search-exposure provenance review using instructor-provided records rests on [301, 2026] and [298, 2026]. The most specific cited work observes: Official Intelligence Community strategy for open-source intelligence governance, integration, source discovery, data, tools, tradecraft, and workforce priorities. Use them for pinning down the scope of **Search-exposure provenance review using instructor-provided records**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **Search-exposure provenance review** against the works cited for this row. [301, 2026] Official Intelligence Community strategy for open-source intelligence governance, integration, source discovery, data, tools, tradecraft, and workforce priorities. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Search-exposure provenance review**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must record the tool-and-terms descriptor, the bounded claim about **Search-exposure provenance review using instructor-provided**, the minimization caveat, the reproducibility uncertainty, the identity-exposure boundary, and the reviewer who approves the use. Shape **Search-exposure provenance review** work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Search-exposure provenance review**: that a source being publicly accessible means collecting it is unrestricted, ungoverned, and free of legal, ethical, and scoping limits.

Transfer task. Transfer **Search-exposure provenance review** from this module to a second motif by preserving least-privilege agent design and run review, replacing action with audit, and naming the blocked use.

50.2.2.3 Lesson 3: Autonomous Vulnerability Scanner: AutoGen + Nmap + MITRE ATT&CK Navigator

Concept. Autonomous Vulnerability Scanner: AutoGen + Nmap + MITRE ATT&CK Navigator treats the vulnerability record as an assurance case: severity, affected component, provenance, mitigation status, and uncertainty stay separate.

Why it matters. Without explicit treatment of **Autonomous Vulnerability Scanner**, excessive agency undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Autonomous Vulnerability Scanner: AutoGen + Nmap + MITRE ATT&CK Navigator rests on [300, 2026], [304, 2026], and [306, 2026]. The most specific cited work observes: NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Use them for fixing what **Autonomous Vulnerability Scanner: AutoGen + Nmap + MITRE ATT&CK Navigator** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Autonomous Vulnerability Scanner**, work from the cited evidence behind this row. [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Autonomous Vulnerability Scanner**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the source descriptor, the bounded claim about **Autonomous Vulnerability Scanner**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Autonomous Vulnerability Scanner** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that Autonomous Vulnerability Scanner: AutoGen + Nmap + MITRE ATT&CK Navigator is optional whenever separate agent assistance from autonomous external action feels inconvenient.

Transfer task. Transfer **Autonomous Vulnerability Scanner** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

50.2.2.4 Lesson 4: RAG Pipeline for All-Source Intelligence Fusion: LangGraph + Chroma + OpenAI

Concept. RAG Pipeline for All-Source Intelligence Fusion: LangGraph + Chroma + OpenAI evaluates retrieval pipelines by source provenance, injection risk, citation fidelity, and reviewer verification of answers.

Why it matters. RAG Pipeline for All-Source Intelligence Fusion connects classroom vocabulary to Agentic AI Governance and Tool Security practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. RAG Pipeline for All-Source Intelligence Fusion: LangGraph + Chroma + OpenAI rests on [305, 2026], [304, 2026], and [303, 2026]. The closest source to this row notes: An official NIST page on software supply chain security issued under Executive Order 14028, focused on the Software Bill of Materials as a formal record of software components and their supply chain. Use them for pinning down the scope of **RAG Pipeline for All-Source Intelligence Fusion: LangGraph + Chroma + OpenAI**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **RAG Pipeline for All-Source Intelligence Fusion** against the works cited for this row. [305, 2026] Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. [303, 2026] An official NIST page on software supply chain security issued under Executive Order 14028, focused on the Software Bill of Materials as a formal record of software components and their supply chain. It explains the benefits of SBOMs for vulnerability identification and supply-chain transparency, recommends machine-readable formats such as SPDX, CycloneDX, and SWID, and describes foundational, sustaining, and enhancing levels of implementation. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **RAG Pipeline for All-Source Intelligence Fusion**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the source descriptor, the bounded claim about **RAG Pipeline for All-Source Intelligence**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **RAG Pipeline for All-Source Intelligence Fusion** work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that RAG Pipeline for All-Source Intelligence Fusion: LangGraph + Chroma + OpenAI establishes intent without reviewing alternative explanations.

Transfer task. Transfer **RAG Pipeline for All-Source Intelligence Fusion** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

50.2.2.5 Lesson 5: Claim-ledger memory exercise that tracks evidence changes rather than people

Concept. Claim-ledger memory exercise that tracks evidence changes rather than people treats agent memory terms as a pedagogical taxonomy unless a domain memory source is cited; MCP and official agentic-AI guidance support external-memory governance, tool boundaries, logs, retention, and reviewer control.

Why it matters. Without explicit treatment of **Claim-ledger memory exercise that tracks evidence changes rather than people**, excessive agency undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Claim-ledger memory exercise that tracks evidence changes rather than people rests on [301, 2026] and [298, 2026]. The lead source's own note reads: Official Intelligence Community strategy for open-source intelligence governance, integration, source discovery, data, tools, tradecraft, and workforce priorities. Use them for the working definition that **Claim-ledger memory exercise that tracks evidence changes rather than people** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Claim-ledger memory exercise that tracks evidence changes rather than people**, reason from the sources cited in this row. [301, 2026] Official Intelligence Community strategy for open-source intelligence governance, integration, source discovery, data, tools, tradecraft, and workforce priorities. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Claim-ledger memory exercise that tracks evidence changes rather than people**, build a claim-ledger memory card with source descriptor, source-change event, retention rule, contamination check, and reviewer disposition; do not track real people, assets, or behavioral patterns. Shape this subject work as an **agent run and assurance card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Claim-ledger memory exercise that tracks evidence changes rather than people**: that a visible feature is enough for a confident geospatial claim.

Transfer task. Reuse the **Claim-ledger memory exercise that tracks evidence changes rather than people** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

50.2.2.6 Lesson 6: Psychological inoculation and prebunking literacy **Concept. Psychological inoculation and prebunking literacy** uses inoculation methods as evidence-informed, bounded, and context-dependent resilience education with transparent labels, source checks, non-manipulative corrections, and explicit measurement limits.

Why it matters. Without explicit treatment of **Psychological inoculation**, treating resilience labels as permission to skip provenance review undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Psychological inoculation and prebunking literacy rests on [308, 2026] and [311, 2026]. Its anchor reference records: It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering. Use them for the working definition that **Psychological inoculation and prebunking literacy** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. For **Psychological inoculation**, work from the cited evidence behind this row. [308, 2026] An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure. [311, 2026] An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. Build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must record the narrative provenance, the bounded claim about **Psychological inoculation**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape this subject work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Psychological inoculation**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **Psychological inoculation** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

50.2.2.7 Lesson 7: Supply Chain Inspector: SBOM + GitHub Commit Analysis + Anomaly Detection **Concept. Supply Chain Inspector: SBOM + GitHub Commit Analysis + Anomaly Detection** shows how package provenance, social trust, build integrity, and assurance controls turn a software incident into reviewable evidence.

Why it matters. Without explicit treatment of **Supply Chain Inspector**, excessive agency undermines least-privilege agent design and run review; the lesson builds the habit to separate agent assistance from autonomous external action.

Source support. Supply Chain Inspector: SBOM + GitHub Commit Analysis + Anomaly Detection rests on [303, 2026], [304, 2026], and [305, 2026]. The most specific cited work observes: An official NIST page on software supply chain security issued under Executive Order 14028, focused on the Software Bill of Materials as a formal record of software components and their supply chain. Use them for the claim that **Supply Chain Inspector: SBOM + GitHub Commit Analysis + Anomaly Detection** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Read **Supply Chain Inspector** against the works cited for this row. [303, 2026] An official NIST page on software supply chain security issued under Executive Order 14028, focused on the Software Bill of Materials as a formal record of software components and their supply chain. It explains the benefits of SBOMs for vulnerability identification and supply-chain transparency, recommends machine-readable formats such as SPDX, CycloneDX, and SWID, and describes foundational, sustaining, and enhancing levels of implementation. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. [305, 2026] Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Supply Chain Inspector**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the source descriptor, the bounded claim about **Supply Chain Inspector**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Supply Chain Inspector** work as an **agent run and assurance card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that Supply Chain Inspector: SBOM + GitHub Commit Analysis + Anomaly Detection is optional whenever separate agent assistance from autonomous external action feels inconvenient.

Transfer task. Transfer **Supply Chain Inspector** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

50.2.2.8 Lesson 8: ICS Anomaly Detection Agent: OT Network + MITRE ATT&CK for ICS **Concept. ICS Anomaly Detection Agent: OT Network + MITRE ATT&CK for ICS** treats agents as software actors with explicit permissions, logs, stop conditions, and human approval—not autonomous decision makers.

Why it matters. Analysts use **ICS Anomaly Detection Agent** to separate agent assistance from autonomous external action. A defensible treatment names the judgment it enables for least-privilege agent design and run review, the proof limit that excessive agency would otherwise hide, and the reviewer accountable for challenge.

Source support. ICS Anomaly Detection Agent: OT Network + MITRE ATT&CK for ICS rests on [307, 2026], [305, 2026], and [304, 2026]. The lead source's own note reads: NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Use them for the claim that **ICS Anomaly Detection Agent: OT Network + MITRE ATT&CK for ICS** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [OECD, 2026a]; [of Canada Secretariat, 2026a].

Evidence to inspect. Ground **ICS Anomaly Detection Agent** in the evidence the row cites. [307, 2026] Official CISA Industrial Control Systems recommended practices page for defensive ICS/OT safety, resilience, and incident-preparation guidance. [305, 2026] Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **ICS Anomaly Detection Agent**, build a **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** for this least-privilege agent design and run review topic. The artifact must name the source descriptor, the bounded claim about **ICS Anomaly Detection Agent**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **ICS Anomaly Detection Agent** work as an **agent run and assurance card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that ICS Anomaly Detection Agent: OT Network + the module establishes intent without reviewing alternative explanations.

Transfer task. Transfer **ICS Anomaly Detection Agent** to a second module by preserving least-privilege agent design and run review, changing the source evidence, and naming a new reviewer.

50.2.3 AGEINT Python Code Library worked safe example: synthetic inputs, evidence, and review

Worked example: a synthetic research assistant agent organizes public readings for an instructor. [242, 2026]; [243, 2026].

Triangulation anchors. In module 36's worked-example section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **governed agentic intelligence**. Learners use a **agent run and assurance card** and keep this boundary visible: No autonomous external action, credentialed operations, live-target workflows, or uncontrolled tool use.

Frame. The classroom question centers on **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII**. Excluded actions stay explicit, and the **Agentic Tool-Governance Lens** planning question is: Which human authority, agent identity, tool permission, autonomy limit, incident threshold, and recoverability condition bounds the workflow?

Inputs. For the **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII** scenario, use public URLs, a fixed retrieval tool, a summarization prompt, a time budget, and a stop condition. The Agentic Tool-Governance Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII**, students bind the agent identity, list allowed tools, set autonomy limits, capture sources, block unsafe requests, and log approvals. Pause whenever an inference about Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII** classroom scenario; unit artifact = agent run and assurance card; evidence = allowed inputs; method = least-privilege agent design and run review; output = an agent run card with tool calls, source links, blocked actions, reviewer notes, incident threshold, and recovery decision; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII** as "Agentic Tool-Governance Lens confirms it" is not enough. The revision ties the claim to least-privilege agent design and run review, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

50.2.4 AGEINT Python Code Library practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Agentic Tool-Governance Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**.

Triangulation anchors. In module 36's practice-sequence section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII, Search-exposure provenance review using instructor-provided records, Autonomous Vulnerability Scanner: AutoGen + Nmap + MITRE ATT&CK Navigator; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Agentic AI Governance and Tool Security** lane.
2. Frame	Answer the lens question: Which human authority, agent identity, tool permission, autonomy limit, incident threshold, and recoverability condition bounds the workflow?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII: agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the agent run and assurance card fields for Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII.	Unit profile note.	Evidence artifacts include tool-allowlist record, external-memory governance boundary.
4. Challenge	Test the misconception that Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII replaces human review whenever evidence looks plausible.	Failure-mode note.	The artifact applies the key distinction: separate agent assistance from autonomous external action.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

50.2.4.1 AGEINT Python Code Library instructor notes: source reasoning, review points, and studio focus

Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human

review point. Keep the focus on **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**. [242, 2026]; [243, 2026].

50.2.4.2 AGEINT Python Code Library extension exercise: peer validation and refresh trigger review **Evidence anchor.** Section 50; [242, 2026].
Have learners swap artifacts and apply the **Agentic Tool-Governance Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**.

50.2.5 AGEINT Python Code Library knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 50; [242, 2026].

1. Explain how **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII** is defined here; name the source descriptor that supports the definition.
2. Contrast **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII** with **Search-exposure provenance review using instructor-provided records** using the **Agentic Tool-Governance Lens** artifact fields.
3. Identify one failure mode from the **Agentic AI Governance and Tool Security** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which permission can be removed while preserving the learning objective?
5. Correct this misconception: that Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII replaces human review whenever evidence looks plausible.

50.2.5.1 AGEINT Python Code Library answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII** without source evidence, uncertainty, or a safe transfer task.

50.3 AGEINT Python Code Library assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 50; [242, 2026].

50.3.1 AGEINT Python Code Library evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 50; [242, 2026].

50.3.2 AGEINT Python Code Library transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 50; [242, 2026].

50.3.2.1 AGEINT Python Code Library lineage and source tradition: profile, concepts, and first anchors This sits in the **Agentic AI Governance and Tool Security** lineage: delegated action under explicit authority, identity, permissions, tool boundaries, monitoring, and human escalation. [242, 2026]; [243, 2026].

50.3.2.2 AGEINT Python Code Library working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 50; [242, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**, with provenance and reviewability throughout.

50.3.2.3 AGEINT Python Code Library knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [242, 2026]; [243, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

50.3.2.4 AGEINT Python Code Library transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 50; [242, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**.
- **Evidence contract:** keep the **Agentic AI Governance and Tool Security** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

50.3.2.5 AGEINT Python Code Library profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 50; [242, 2026].

The matched profile emphasizes delegated action under explicit authority, identity, permissions, tool boundaries, monitoring, and human escalation. The method stack is AI RMF Govern-Map-Measure-Manage, least-privilege tool design, prompt-injection review, progressive deployment, and rollback drills; the local topic cluster is **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**.

50.3.3 AGEINT Python Code Library evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 50; [242, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Agentic AI Governance and Tool Security** profile tells reviewers what evidence is strong enough for the module artifact built around **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**.

50.3.3.1 AGEINT Python Code Library guide source spine: inherited keys and local citation roles Primary guide citations: [242, 2026]; [243, 2026]; [246, 2026]; [280, 2026]; [281, 2026]; [282, 2026]; [292, 2026]; [295, 2026]; [296, 2026]; [299, 2026]; [306, 2026]; [312, 2026]; [309, 2026]; [310, 2026]; [300, 2026]; [304, 2026]; [303, 2026]; [305, 2026]; [307, 2026]; [301, 2026]; [298, 2026]; [308, 2026]; [311, 2026].

50.3.3.2 AGEINT Python Code Library verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [242, 2026]; [243, 2026].

Tier	What counts	How it is used
Source guide	[242, 2026]; [243, 2026]; [246, 2026]; [280, 2026]; [281, 2026]; [282, 2026]; [292, 2026]; [295, 2026]; [296, 2026]; [299, 2026]; [306, 2026]; [312, 2026]; [309, 2026]; [310, 2026]; [300, 2026]; [304, 2026]; [303, 2026]; [305, 2026]; [307, 2026]; [301, 2026]; [298, 2026]; [308, 2026]; [311, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 36's source-canon section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records** and [242, 2026]; [243, 2026], but only directly verified source URLs are encoded as citations.

50.3.3.3 AGEINT Python Code Library intelligence practice lens: evidence artifact and safety check Practice lens: **Agentic Tool-Governance Lens** for **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**. [242, 2026]; [243, 2026].

Planning question: Which human authority, agent identity, tool permission, autonomy limit, incident threshold, and recoverability condition bounds the workflow?

Evidence artifact: agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path.

Validation rule: verify least privilege, prompt-injection exposure, provenance, observability, stop conditions, and incident-reporting triggers. Applied to **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**.

Handoff contract: export agent traces, tool calls, retrieved sources, policy decisions, and human approvals separately.

Safety check: block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions.

50.3.3.4 AGEINT Python Code Library runtime-to-reader map: generated sections and verifier surfaces **Evidence anchor.** Section 50; [242, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	36.99	36.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind AGEINT Python Code Library to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
AGEINT pattern registry, agent identity, and interface-contract studio	36.100	36.100 source title transformed into safe curriculum treatment; original: V2 AGEINT-depth extension: convert code-library material into education-safe capstone workflows with instructor rubrics, prompt transparency, allowed tools, and human override requirements	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Bounded autonomy, procurement, incident-response, and assurance studio	36.101	36.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for AGEINT Python Code Library	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Model-card, recoverability, retention, and learner-support evidence package	36.102	36.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for AGEINT Python Code Library	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII	36.1	36.1 Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Search-exposure provenance review using instructor-provided records	36.2	36.2 source title transformed into safe curriculum treatment; original: Multi-Agent OSINT Crew: CrewAI + Shodan + theHarvester + Maltego	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Autonomous Vulnerability Scanner: AutoGen + Nmap + MITRE ATT&CK Navigator	36.3	36.3 Autonomous Vulnerability Scanner: AutoGen + Nmap + MITRE ATT&CK Navigator	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
RAG Pipeline for All-Source Intelligence Fusion: LangGraph + Chroma + OpenAI	36.4	36.4 RAG Pipeline for All-Source Intelligence Fusion: LangGraph + Chroma + OpenAI	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Claim-ledger memory exercise that tracks evidence changes rather than people	36.5	36.5 source title transformed into safe curriculum treatment; original: Pattern-of-Life Analysis Agent: Persistent Memory + GEOINT + OSINT	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Psychological inoculation and prebunking literacy	36.6	36.6 source title transformed into safe curriculum treatment; original: Cognitive Security Inoculation Agent: Van der Linden Taxonomy + GPT-4o	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Supply Chain Inspector: SBOM + GitHub Commit Analysis + Anomaly Detection	36.7	36.7 Supply Chain Inspector: SBOM + GitHub Commit Analysis + Anomaly Detection	Software-Supply-Chain Assurance Lens	software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps	exclude exploit reproduction, maintainer targeting, backdoor mechanics, credential hunting, and live repository interference
ICS Anomaly Detection Agent: OT Network + MITRE ATT&CK for ICS	36.8	36.8 ICS Anomaly Detection Agent: OT Network + MITRE ATT&CK for ICS	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

50.3.3.5 AGEINT Python Code Library reusable subsection contract: topic rows, artifacts, and safety duties **Evidence anchor.** Section 50; [242, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Search-exposure provenance review using instructor-provided records	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Autonomous Vulnerability Scanner: AutoGen + Nmap + MITRE ATT&CK Navigator	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
RAG Pipeline for All-Source Intelligence Fusion: LangGraph + Chroma + OpenAI	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Claim-ledger memory exercise that tracks evidence changes rather than people	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Psychological inoculation and prebunking literacy	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions
Supply Chain Inspector: SBOM + GitHub Commit Analysis + Anomaly Detection	Software-Supply-Chain Assurance Lens	software-supply-chain assurance packet with package provenance, maintainer-risk notes, build-integrity evidence, and control gaps	exclude exploit reproduction, maintainer targeting, backdoor mechanics, credential hunting, and live repository interference
ICS Anomaly Detection Agent: OT Network + MITRE ATT&CK for ICS	Agentic Tool-Governance Lens	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path	block excessive agency, shadow tools, credential leakage, autonomous deployment, and irreversible actions

50.3.3.6 AGEINT Python Code Library annotated source ledger: real titles and local contribution Each source cited by this **Agentic AI Governance and Tool Security** module is paired below with its real title and a one-line note on what it contributes to **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**.

Source	Cited work	What it contributes	Status
[242, 2026]	Guidance for Generative AI in Education and Research	Official UNESCO generative AI education guidance.	original source-guide
[243, 2026]	AI Competency Frameworks for Teachers and Students	A UNESCO announcement of two new AI competency frameworks, one for students and one for teachers, intended to guide safe and responsible engagement with artificial intelligence in education. The student framework emphasizes a human-centered perspective, ethical use, foundational AI knowledge, and design thinking, while the teacher framework covers ethics, technical understanding, and pedagogy.	verified source-guide
[246, 2026]	Digital Education Action Plan 2021-2027	The European Commission's official page on the Digital Education Action Plan (2021-2027), a strategic framework for promoting high-quality, inclusive digital learning across EU education systems. It defines digital education as the use of digital tools, technologies, and content to support teaching, learning, and assessment, and cites pandemic-driven adoption alongside persistent gaps in teacher readiness, student digital skills, and household access.	verified source-guide

Source	Cited work	What it contributes	Status
[280, 2026]	NIST SP 800-61 Rev. 3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management	NIST SP 800-61 Rev. 3, published April 2025, integrates incident response guidance into broader cybersecurity risk management aligned with the NIST Cybersecurity Framework 2.0, superseding the 2012 Rev. 2. The publication addresses cyber threat information sharing, incident handling and management practices, and procedures for detecting, responding to, and recovering from security incidents.	verified source-guide
[281, 2026]	Artificial Intelligence Cybersecurity Challenges	An ENISA (European Union Agency for Cybersecurity) report published December 15, 2020 mapping the cybersecurity challenges of artificial intelligence. It defines AI scope through a lifecycle approach, identifies the assets requiring protection within AI ecosystems, and develops a threat taxonomy classified across lifecycle stages and asset categories.	verified source-guide
[282, 2026]	AI Research: Security and Resilience	A NIST page on AI research focused on security and resilience, framing these as core characteristics of trustworthy AI under the NIST AI Risk Management Framework.	verified source-guide
[292, 2026]	Assessing Risks and Impacts of AI (ARIA): Pilot Evaluation Report	The ARIA 0.1 pilot evaluation report documents NIST's methodology for systematically assessing AI applications for risks and societal impacts, using a multi-layered evaluation approach across five participating organizations and seven submitted AI applications. The pilot employed three evaluation scenarios and three testing levels: model testing, red teaming, and field testing, supplemented by dialogue annotation, tester questionnaires, and structured measurement trees.	verified source-guide
[295, 2026]	M-25-22: Driving Efficient Acquisition of Artificial Intelligence in Government	OMB Memorandum M-25-22 (April 3, 2025), Driving Efficient Acquisition of Artificial Intelligence in Government, issued under Executive Order 13960 and related directives. It provides guidance to federal agencies for acquiring effective and trustworthy AI in a timely, cost-effective manner, and rescinds and replaces earlier memorandum M-24-18.	verified source-guide
[296, 2026]	Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile	NIST AI 600-1, the Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, a cross-sectoral companion resource to the NIST AI RMF 1.0 issued pursuant to Executive Order 14110. It identifies risks that are unique to or amplified by generative AI and organizes suggested actions for managing those risks, mapped to the AI RMF functions.	verified source-guide

Source	Cited work	What it contributes	Status
[299, 2026]	Model Context Protocol Specification	The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation).	verified source-guide context; use pinned MCP anchor for normative claims
[306, 2026]	Artificial Intelligence	Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support.	original source-guide
[312, 2026]	Guide on the Use of Agentic Artificial Intelligence	Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support.	original source-guide
[309, 2026]	STIX Version 2.1	An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection.	verified source-guide
[310, 2026]	TAXII Version 2.1	The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe).	verified source-guide
[300, 2026]	MITRE ATLAS	MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy.	original source-guide
[304, 2026]	Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities	NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences.	verified source-guide
[303, 2026]	Software Security in Supply Chains	An official NIST page on software supply chain security issued under Executive Order 14028, focused on the Software Bill of Materials as a formal record of software components and their supply chain. It explains the benefits of SBOMs for vulnerability identification and supply-chain transparency, recommends machine-readable formats such as SPDX, CycloneDX, and SWID, and describes foundational, sustaining, and enhancing levels of implementation.	verified source-guide

Source	Cited work	What it contributes	Status
[305, 2026]	DevSecOps	Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support.	original source-guide
[307, 2026]	ICS Recommended Practices	Official CISA Industrial Control Systems recommended practices page for defensive ICS/OT safety, resilience, and incident-preparation guidance.	original source-guide
[301, 2026]	The IC OSINT Strategy 2024-2026	Official Intelligence Community strategy for open-source intelligence governance, integration, source discovery, data, tools, tradecraft, and workforce priorities.	original source-guide
[298, 2026]	Intelligence Community Directives	Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations.	original source-guide
[308, 2026]	Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure	An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure.	verified source-guide
[311, 2026]	Countering Information Threats	An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering.	verified source-guide

Where this sits. This module's overview is Section 50; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

50.3.4 AGEINT Python Code Library governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 50; [242, 2026].

50.3.5 AGEINT Python Code Library analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 36's governance-boundary section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Research lane: **Agentic AI Governance and Tool Security** for **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**. [242, 2026]; [243, 2026].
Curriculum topic spine: Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII, **Search-exposure provenance review using instructor-provided records**, **Autonomous Vulnerability Scanner: AutoGen + Nmap + MITRE ATT&CK Navigator**. **Verified anchor cluster:** [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]; [Community, 2020b]; [Community, 2020a]; [of the Director of National Intelligence, 2025b].
Conceptual depth: delegated action under explicit authority, identity, permissions, tool boundaries, monitoring, and human escalation.
Method stack: AI RMF Govern-Map-Measure-Manage, least-privilege tool design, prompt-injection review, progressive deployment, and rollback drills.
Composability contract: agents, tools, credentials, memory, retrieval stores, policies, and logs remain separately inspectable and revocable components.
Known failure modes: excessive agency, shadow tools, indirect prompt injection, memory poisoning, confused authority, and unbounded action chains.
Defensive boundary: agentic workflows stay synthetic, owned-lab, supervised, logged, rate-limited, and reversible unless a lawful production authority exists. Applied to **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**.

Anchor	Why it matters here
[OECD, 2026a]	Official OECD conceptual foundation for agentic AI. Checked as of 2026-05-21; role: source_quality_anchor.
[of Canada Secretariat, 2026a]	Government of Canada guide for accountable public-sector use of agentic AI, including governance, risk, transparency, testing, monitoring, and human oversight considerations. Checked as of 2026-05-24; role: curriculum_anchor.
[of Standards and Technology, 2023]	Official NIST.AI.100-1 risk-management framework. Checked as of 2026-05-21; role: source_quality_anchor.
[of Standards and Technology, 2024d]	Official NIST AI 600-1 generative AI profile. Checked as of 2026-05-21; role: source_quality_anchor.
[Community, 2020b]	Official IC principles for lawful, accountable, objective, human-centered, secure, resilient, and science-informed AI. Checked as of 2026-05-21; role: curriculum_anchor.
[Community, 2020a]	Official IC framework for AI goals, authorities, human judgment, bias mitigation, testing, documentation, explainability, and review. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2025b]	Official IC AI governance directive covering CAIO roles, oversight, interoperability, civil-liberties review, training data, and impact assessment. Checked as of 2026-05-21; role: curriculum_anchor.

50.3.5.1 AGEINT Python Code Library evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **Agentic AI Governance and Tool Security** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [242, 2026]; [243, 2026].

50.3.6 AGEINT Python Code Library agentic boundary: assist, approve, block, and record

Evidence anchor. Section 50; [242, 2026].
AGEINT translation is bounded by the **Agentic AI Governance and Tool Security** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**.

50.3.6.1 AGEINT Python Code Library permitted defensive utility: curriculum uses and safe outputs

Evidence anchor. Section 50; [242, 2026].
The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**.

50.3.6.2 AGEINT Python Code Library excluded operational boundary: blocked actions and stop rules

Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [242, 2026]; [243, 2026] and **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

50.3.7 AGEINT Python Code Library governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 50; [242, 2026].
Governance is practiced as a gate on the **Agentic AI Governance and Tool Security** lane. Learners use the **Agentic Tool-Governance Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**.

50.3.7.1 AGEINT Python Code Library governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [242, 2026]; [243, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Agentic AI Governance and Tool Security** failure modes and the **Agentic Tool-Governance Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

50.3.7.2 AGEINT Python Code Library evidence package handoff: appendices, records, and reuse **Evidence anchor.** Section 50; [242, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Agentic Tool-Governance Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**.

50.3.7.3 AGEINT Python Code Library current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**. [242, 2026]; [243, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_oecd_agentic_ai` for **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**?	The Agentic AI Landscape and Its Conceptual Foundations; lane `source_quality_spine`; checked 2026-05-21.	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path; Official OECD conceptual foundation for agentic AI.
What does the module inherit from `official_canada_agentic_ai_guide` for **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**?	Guide on the Use of Agentic Artificial Intelligence; lane `public_sector_agentic_ai`; checked 2026-05-24.	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path; bounded-autonomy run card, recoverability review, approval threshold, monitoring evidence, and public-sector service assurance
What does the module inherit from `official_nist_ai_rmf` for **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**?	Artificial Intelligence Risk Management Framework (AI RMF 1.0); lane `source_quality_spine`; checked 2026-05-21.	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path; Official NIST.AI.100-1 risk-management framework.
What does the module inherit from `official_nist_ai_600_1` for **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**?	Artificial Intelligence Risk Management Framework: Generative AI Profile; lane `source_quality_spine`; checked 2026-05-21.	agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path; Official NIST AI 600-1 generative AI profile.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 50; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

50.3.8 AGEINT Python Code Library assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 50; [242, 2026].

50.3.9 AGEINT Python Code Library assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 50; [242, 2026].

50.3.9.1 AGEINT Python Code Library capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records** and [242, 2026]; [243, 2026].

50.3.9.2 AGEINT Python Code Library instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records** and [242, 2026]; [243, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

50.3.9.3 AGEINT Python Code Library assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII	Completed **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Search-exposure provenance review using instructor-provided records	Completed **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Autonomous Vulnerability Scanner: AutoGen + Nmap + MITRE ATT&CK Navigator	Completed **agent run card with tool allowlist, identity, logs, autonomy limit, approval gates, and recovery path** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

50.3.10 AGEINT Python Code Library refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [242, 2026]; [243, 2026] and **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**.

50.3.10.1 AGEINT Python Code Library refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**. The local signals begin with [242, 2026]; [243, 2026].

50.3.10.2 AGEINT Python Code Library claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**, and the source spine for these checks begins with [242, 2026]; [243, 2026].

50.3.11 AGEINT Python Code Library reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [242, 2026]; [243, 2026].

Triangulation anchors. In module 36's review-checklist section, directly verified anchors for the **Agentic AI Governance and Tool Security** lane include [OECD, 2026a]; [of Canada Secretariat, 2026a]; [of Standards and Technology, 2023]; [of Standards and Technology, 2024d]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records**. [242, 2026]; [243, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.

- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

50.3.12 AGEINT Python Code Library learning-path links: module map, overview, and curriculum atlas

Use the cross-links below to place **Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII; Search-exposure provenance review using instructor-provided records** in the wider unit: the orientation sets the frame, the parent unit supplies the shared safety posture, and the neighbouring modules show what evidence enters and leaves. Lead sources: [242, 2026]; [243, 2026].

Section 2, Section 44, Section 49, Section 51

51 COGNITIVE SECURITY

51.1 COGNITIVE SECURITY learning spine and source route: unit purpose, module order, and evidence handoff

Evidence anchor. Section 51; [238, 2026].

51.1.1 cognitive resilience and epistemic integrity discipline spine: domain question and learning focus

Evidence anchor. Section 51; [238, 2026].
This unit teaches **cognitive resilience and epistemic integrity**. Cognitive-security lessons protect attention, trust, memory, and judgment by tracing provenance, correction paths, and transparent education.

51.1.2 cognitive resilience and epistemic integrity source-use contract: citation roles and evidence limits

Evidence anchor. Section 51; [238, 2026].
Use CISA, NATO, and analytic-tradecraft anchors for influence mitigation, information-threat analysis, and confidence discipline.

51.1.3 cognitive resilience and epistemic integrity practice artifact: recurring packet and retained evidence

Evidence anchor. Section 51; [238, 2026].
The recurring practice artifact is a **epistemic-integrity review packet** that draws on provenance chain, correction option, harm note, and confidence language. The unit keeps its learning spine explicit. Learners separate narrative spread from intent, document uncertainty, and choose transparent resilience moves.

51.1.4 cognitive resilience and epistemic integrity safety boundary: accountable, synthetic, and evidence-bounded limits

No manipulation, covert persuasion, medicalized claims, or population-level targeting.
This unit introduces the part's governing question, evidence artifacts, source-support spine, and capstone thread before the individual modules begin. [238, 2026]; [239, 2026].
Learners carry one unit capstone thread through the part: define an accountable intelligence question, bind it to source-quality constraints, produce a reviewable artifact, test the artifact against failure modes, and hand it off with enough context for another analyst or instructor to audit. The capstone remains public, synthetic, or owned-lab throughout; its first source anchors are [238, 2026]; [239, 2026].
This unit's deliverables are a source-canon card, claim/evidence ledger, safe-practice lab packet, failure-mode note, instructor rubric, and debrief memo. The full source-lane and evidence-package ledgers appear in the orientation and appendices; this unit introduction keeps only the learner-facing spine for [238, 2026]; [239, 2026].
This unit's safety gates are scope authorization, rights review, data provenance, tool allowlisting, human oversight, rollback, and evidence-bounded output. A missing gate turns the activity into a tabletop, audit, or written governance exercise until the gate is restored against [238, 2026]; [239, 2026].
Capstone thread:

Phase	Artifact	Review gate
Question	accountable learning question and excluded-action list	instructor confirms scope, allowed data, and rights impact
Source canon	source-lane map with guide citations, verified anchors, and refresh dates	citation keys resolve and source identity lock remains stable
Evidence ledger	claim, evidence, uncertainty, confidence, and reviewer register	every material claim has a source, caveat, and owner
Safe lab	synthetic or public dataset packet, tool allowlist, and stop conditions	no live target, private data, external action, or unsafe cyber-physical step
Assurance	evaluation rubric, failure-mode drill, rights map, and remediation note	human reviewer signs off before presentation or reuse
Debrief	capstone memo with lessons, residual risk, refresh triggers, and handoff owner	all unresolved questions and future approvals are explicit

Research lane: Cognitive Security and Influence Resilience. Core anchors: [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]. Conceptual focus: protecting attention, belief formation, and decision quality without turning resilience education into manipulation. Composability contract: separate descriptive analysis, normative assessment, response options, and protected-audience considerations. **Practice lens:** Cognitive-Resilience Lens; How does the module protect autonomy, attention, trust, and decision quality without designing persuasion? [238, 2026]; [239, 2026].

51.2 How adversaries target cognition

This unit is organized around the NATO/INSS reconception of cognitive warfare, summarized for the unit in Figure 108, which distinguishes three layers of engagement by their target. The biological layer targets cognitive capacity itself through neuroscience-informed pressure on the nervous system, with AI optimizing delivery timing and channel selection. The psychological layer targets cognitive interpretation, manipulating individual cognition and exploiting biases at scale, with AI tailoring influence to vulnerability profiles. The social layer targets cognitive cohesion, fracturing shared narratives and weaponizing identity to manufacture epistemic chaos, with AI coordinating synthetic influence across platforms [of Excellence, 2026]. Holding the three layers apart matters because each demands a different defense – resilience of attention, inoculation against manipulation, and protection of shared sense-making – and a defender who conflates them will mismatch the countermeasure to the attack. Every exercise in this unit stays defensive, synthetic, and evidence-bounded: the taxonomy is taught to build inoculation and detection, never to script influence [Agency, 2024a].

51.2.1 COGNITIVE SECURITY visual navigation and module map: evidence flow, order, and safety cues

The unit uses Figure 107, Figure 108, Figure 109, and Figure 110 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 50, Section 52.

51.2.2 COGNITIVE SECURITY module roster and source-lane inventory: citations, lanes, and learner route

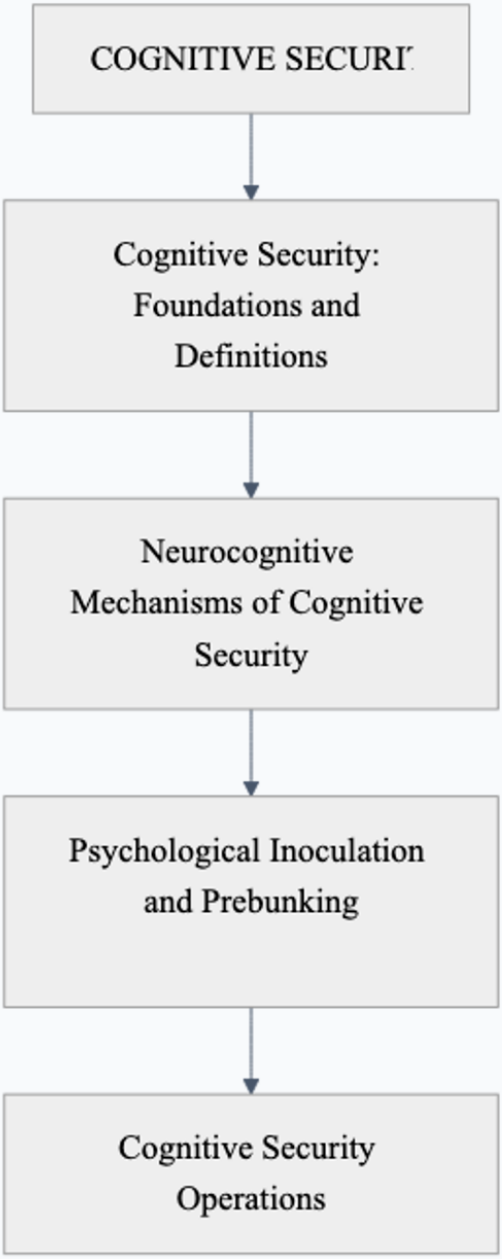


Figure 107: The unit module map traces the part's chapters as a linear reading sequence. The captioned view belongs to the cognitive security section and should be read as a map of 4 module nodes in the unit's ordered, source-backed reading sequence from its first module to its last, not as a capability score or live-task instruction.

Figure 108: The NATO/INSS cognitive warfare taxonomy distinguishes biological, psychological, and social attack layers by their target, mechanism, and the role AI plays in each. The captioned view belongs to the cognitive security section and should be read as a map of NATO/INSS Cognitive Warfare 2026 three layers of engagement, Biological layer, Target cognitive capacity, and Mechanism neuroscience-informed targeting of the nervous system, not as a capability score or live-task instruction.

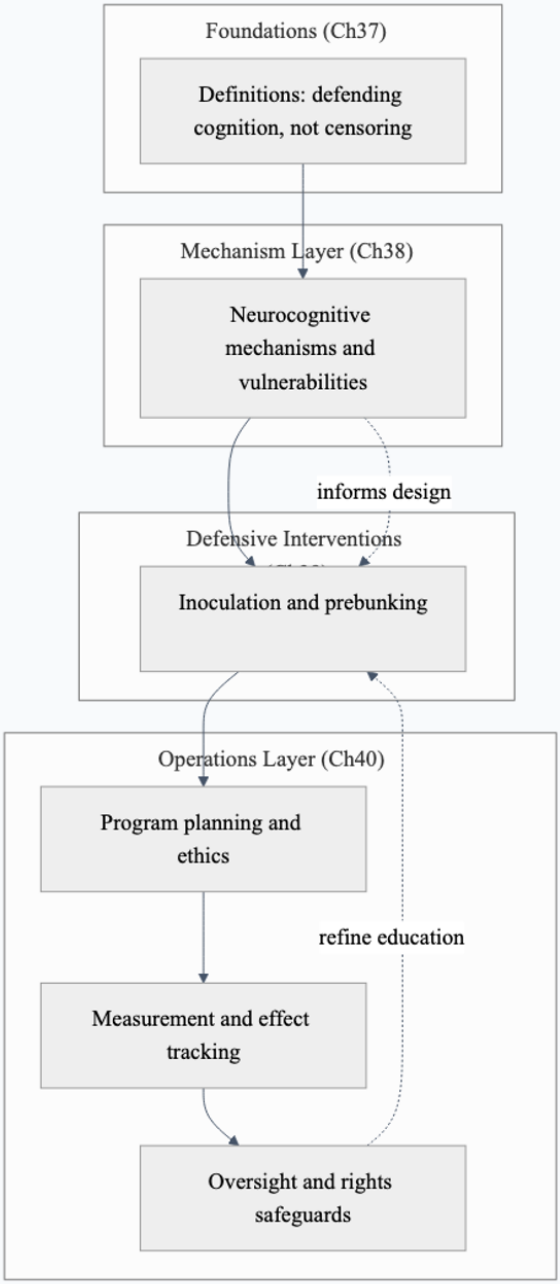


Figure 109: Conceptual part map moving from cognitive-defense definitions through neurocognitive mechanisms and bounded prebunking education into governed operations where measurement and rights safeguards feed back to refine education design. Its reader value is to make Foundations (Ch37), Definitions: defending cognition, not censoring, Mechanism Layer (Ch38), and Neurocognitive mechanisms and vulnerabilities visible at a glance, with the cognitive security section as the source section and defensive review as the boundary.

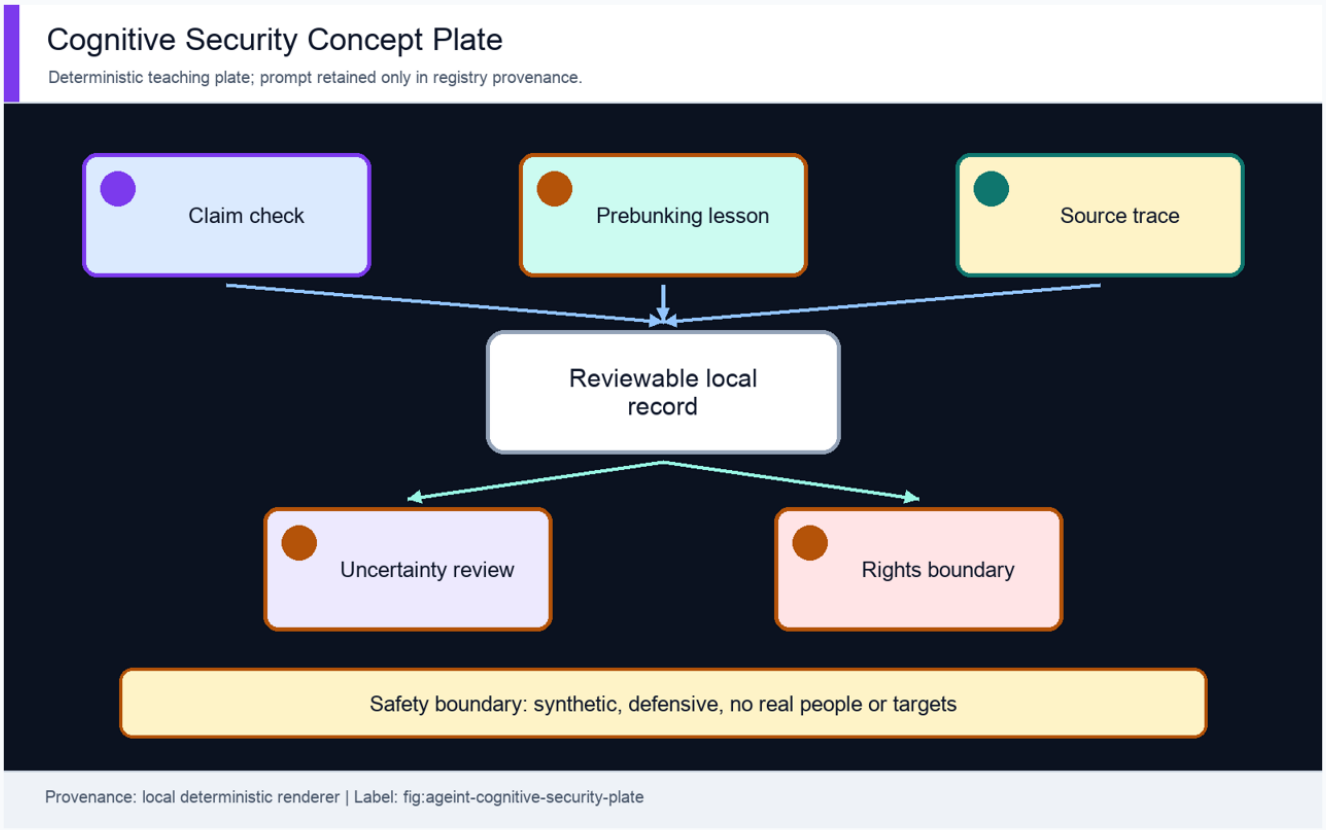


Figure 110: Deterministic teaching plate for cognitive security as defensive inoculation, provenance tracking, and uncertainty management. In the cognitive security section, it lets readers compare Claim check, Prebunking lesson, Source trace, and Uncertainty review so the visual functions as a traceable course aid rather than an unscoped assertion.

Module	Section reference	Source spine
Cognitive Security: Foundations and Definitions	Section 52	[238, 2026]; [239, 2026]; [244, 2026]; [273, 2026]; [276, 2026]; [285, 2026]; [286, 2026]; [290, 2026]; [294, 2026]; [165, 2026]; [166, 2026]; [167, 2026]; [095, 2026]; [096, 2026]; [168, 2026]; [169, 2026]; [170, 2026]; [171, 2026]; [107, 2026]; [172, 2026]; [173, 2026]; [174, 2026]; [175, 2026]; [001, 2026]; [307, 2026]; [305, 2026]; [304, 2026].
Neurocognitive Mechanisms of Cognitive Security	Section 53	[238, 2026]; [240, 2026]; [244, 2026]; [274, 2026]; [278, 2026]; [280, 2026]; [287, 2026]; [288, 2026]; [295, 2026]; [176, 2026]; [177, 2026]; [178, 2026]; [179, 2026]; [180, 2026]; [308, 2026]; [311, 2026].
Psychological Inoculation and Prebunking	Section 54	[242, 2026]; [243, 2026]; [245, 2026]; [279, 2026]; [282, 2026]; [284, 2026]; [289, 2026]; [291, 2026]; [296, 2026]; [181, 2026]; [182, 2026]; [183, 2026]; [152, 2026]; [184, 2026]; [185, 2026]; [186, 2026]; [187, 2026]; [151, 2026]; [308, 2026]; [311, 2026].
Cognitive Security Operations	Section 55	[238, 2026]; [239, 2026]; [246, 2026]; [275, 2026]; [276, 2026]; [283, 2026]; [286, 2026]; [293, 2026]; [295, 2026]; [095, 2026]; [105, 2026]; [188, 2026]; [106, 2026]; [003, 2026]; [096, 2026]; [300, 2026]; [304, 2026]; [306, 2026].

52 Cognitive Security: Foundations and Definitions

52.0.1 Cognitive Security: Foundations and Definitions figures and course links: visual evidence, source flow, and navigation

The module uses Figure 111 and Figure 107 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 51, Section 53.
This module teaches the **Cognitive Security and Influence Resilience** lane through a bounded, source-backed coursebook chapter. [238, 2026]; [239, 2026].

52.1 Cognitive Security and Influence Resilience frame for Cognitive Security: Foundations and Definitions: source context, topic focus, and reader task

Evidence anchor. Section 52; [238, 2026].

52.1.1 Cognitive Security: Foundations and Definitions orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 52; [238, 2026].

52.1.2 Cognitive Security: Foundations and Definitions conceptual primer: source context, core model, and reader task

This chapter teaches cognitive security as protection of attention, trust, memory, and decision quality without creating manipulation. The chapter uses **Cognitive-Resilience Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**.
The central distinction is to separate analysis of influence from persuasion design. Core topics include **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence; Cognitive Security vs. Cybersecurity vs. Information Security**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [238, 2026]; [239, 2026].
Learners move from vocabulary and the **Cognitive-Resilience Lens** distinction through topic lessons on **Cognitive security definitions and scope** with evidence and misconception checks, then assemble a **narrative-risk map with provenance, uncertainty, audience harms, and response options** with safety and rights gates.

52.1.3 Cognitive Security: Foundations and Definitions learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 52; [238, 2026].

- Connect **Cognitive security definitions and scope and Comprehensive Definition: State and Process Against Malign Influence** to **Cognitive Security and Influence Resilience** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate analysis of influence from persuasion design; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as counter-messaging as manipulation, overclaiming intent, pathologizing audiences, and collapsing uncertainty into moral certainty, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: practice uses benign simulations and resilience education; it does not create persuasion campaigns, impersonation, or deception plans.

52.1.4 Cognitive Security: Foundations and Definitions core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 52; [238, 2026].

Term	Working definition
Narrative provenance	where a claim, frame, or story came from and how it spread
Prebunking	transparent education that helps people recognize misleading patterns before exposure
Audience harm	a privacy, dignity, autonomy, or trust risk for people receiving information
Attribution caution	the rule that intent and origin claims need strong evidence
Resilience response	a transparent education, correction, or process improvement that avoids manipulation
MISO boundary	the line between accountable public messaging analysis and covert influence design
Inoculation	building recognition of manipulation tactics without deploying persuasion against a population
Cognitive security definitions and scope	Key terms: Cognitive, security, definitions.
Comprehensive Definition: State and Process…	Key terms: Comprehensive, Definition, State.

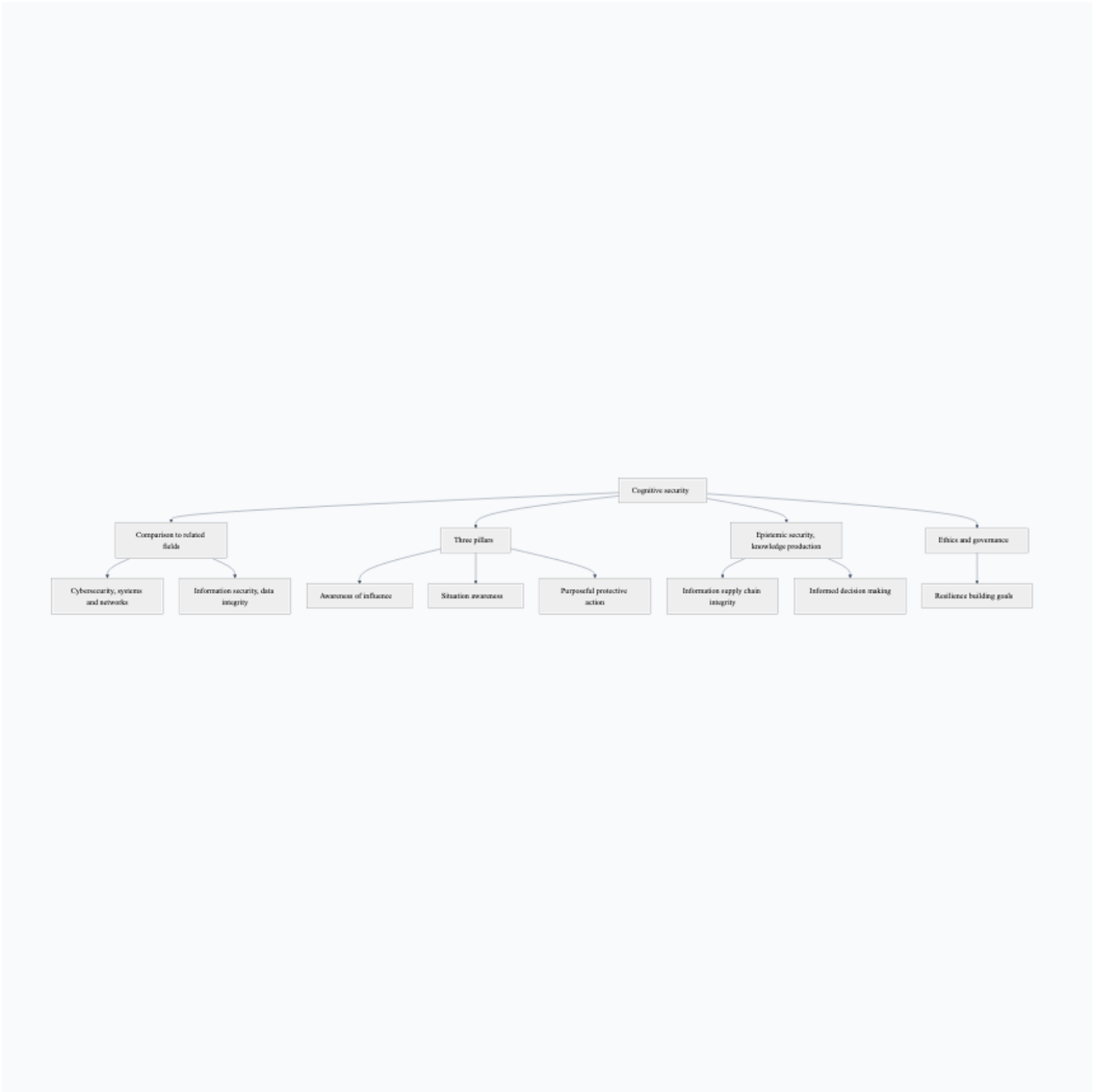


Figure 111: A taxonomy distinguishing cognitive security from related security fields and locating its three pillars and neighboring concept of epistemic security. It is anchored to the cognitive security / cognitive security foundations and definitions section; use it to inspect Cognitive security, Comparison to related fields, Cybersecurity, systems and networks, and Information security, data integrity while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

52.2 Cognitive-Resilience Lens path for Cognitive Security: Foundations and Definitions: lesson cluster, safe artifact, and review

Evidence anchor. Section 52; [238, 2026].

52.2.1 Cognitive Security: Foundations and Definitions practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 52; [238, 2026].

52.2.2 Cognitive Security: Foundations and Definitions topic lessons: source-backed concepts and transfer tasks

This module builds cognitive security as protection of attention, trust, memory, and decision quality without creating manipulation. The sequence opens with **Cognitive security definitions and scope**, **Comprehensive Definition: State and Process Against Malign Influence**, **Cognitive Security vs. Cybersecurity vs. Information Security** and applies the **Cognitive-Resilience Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 107; module overview Section 52; curriculum atlas Section 2.

Triangulation anchors. In module 37's topic-lessons section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

52.2.2.1 Lesson 1: Cognitive security definitions and scope **Concept. Cognitive security definitions and scope** maps cognitive attack surfaces: attention, belief formation, narrative provenance, and transparent correction options.

Why it matters. Analysts use **Cognitive security definitions** to separate analysis of influence from persuasion design. A defensible treatment names the judgment it enables for information-integrity analysis and resilience education review, the proof limit that treating resilience labels as permission to skip provenance review would otherwise hide, and the reviewer accountable for challenge.

Source support. Cognitive security definitions and scope rests on [165, 2026], [166, 2026], and [167, 2026]. The most specific cited work observes: A LinkedIn post by Fran Casino announcing a research article titled 'Unveiling the multifaceted concept of cognitive security: Trends, perspectives, and future challenges,' published in the Elsevier journal Technology in Society. Use them for fixing what **Cognitive security definitions and scope** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Cognitive security definitions**, work from the cited evidence behind this row. [165, 2026] We provide a comprehensive review of the current state of cognitive security. [166, 2026] Cognitive security, as an emerging field. [167, 2026] A LinkedIn post by Fran Casino announcing a research article titled 'Unveiling the multifaceted concept of cognitive security: Trends, perspectives, and future challenges,' published in the Elsevier journal Technology in Society. The post describes the work as a literature review that analyzes definitions, challenges, and future trends in cognitive security and proposes a redefinition based on the concept's core components. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. Build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Cognitive security definitions**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape this subject work as an **epistemic-integrity review packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Cognitive security definitions**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Transfer **Cognitive security definitions** from this module to a second motif by preserving information-integrity analysis and resilience education, replacing action with audit, and naming the blocked use.

52.2.2.2 Lesson 2: Comprehensive Definition: State and Process Against Malign Influence **Concept. Comprehensive Definition: State and Process Against Malign Influence** protects knowledge production with provenance, dissent channels, and transparent correction—not narrative control.

Why it matters. Analysts use **Comprehensive Definition** to separate analysis of influence from persuasion design. A defensible treatment names the judgment it enables for information-integrity analysis and resilience education review, the proof limit that treating resilience labels as permission to skip provenance review would otherwise hide, and the reviewer accountable for challenge.

Source support. Comprehensive Definition: State and Process Against Malign Influence rests on [166, 2026]. Its anchor reference records: Cognitive security, as an emerging field. Use it for fixing what **Comprehensive Definition: State and Process Against Malign Influence** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Read **Comprehensive Definition** against the works cited for this row. [166, 2026] Cognitive security, as an emerging field. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Comprehensive Definition**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Comprehensive Definition**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Comprehensive Definition** work as an **epistemic-integrity review packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Comprehensive Definition**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Transfer **Comprehensive Definition** from this module to a second motif by preserving information-integrity analysis and resilience education, replacing action with audit, and naming the blocked use.

52.2.2.3 Lesson 3: Cognitive Security vs. Cybersecurity vs. Information Security **Concept. Cognitive Security vs. Cybersecurity vs. Information Security** maps cognitive attack surfaces: attention, belief formation, narrative provenance, and transparent correction options.

Why it matters. Without explicit treatment of **Cognitive Security vs. Cybersecurity vs. Information Security**, treating resilience labels as permission to skip provenance review undermines information-integrity analysis and resilience education review; the lesson builds the habit to separate analysis of influence from persuasion design.

Source support. Cognitive Security vs. Cybersecurity vs. Information Security rests on [095, 2026]. The most specific cited work observes: This policy paper examines the emergence of cognitive security. Use it for the working definition that **Cognitive Security vs. Cybersecurity vs. Information Security** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Cognitive Security vs. Cybersecurity vs. Information Security**, work from the cited evidence behind this row. [095, 2026] This policy paper examines the emergence of cognitive security. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Cognitive Security vs. Cybersecurity vs. Information Security**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Cognitive Security vs Cybersecurity vs**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape this subject work as an **epistemic-integrity review packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Cognitive Security vs. Cybersecurity vs. Information Security**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Apply this module's safe boundary for **Cognitive Security vs. Cybersecurity vs. Information Security** to another artifact while keeping information-integrity analysis and resilience education and reviewer ownership explicit.

52.2.2.4 Lesson 4: Three Pillars: Awareness + Situation Awareness + Purposeful Action

Concept. Three Pillars: Awareness + Situation Awareness + Purposeful Action focuses on transparent resilience education: provenance, audience harm, attribution caution, and non-manipulative response options.

Why it matters. Three Pillars connects classroom vocabulary to Cognitive Security and Influence Resilience practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Three Pillars: Awareness + Situation Awareness + Purposeful Action rests on [166, 2026]. The closest source to this row notes: Cognitive security, as an emerging field. Use it for the working definition that **Three Pillars: Awareness + Situation Awareness + Purposeful Action** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Read **Three Pillars** against the works cited for this row. [166, 2026] Cognitive security, as an emerging field. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Three Pillars**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Three Pillars**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Three Pillars** work as an **epistemic-integrity review packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Three Pillars**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Apply this module's safe boundary for **Three Pillars** to another artifact while keeping information-integrity analysis and resilience education and reviewer ownership explicit.

52.2.2.5 Lesson 5: Unveiling the Multifaceted Concept of Cognitive Security (Elsevier, 2025)

Concept. Unveiling the Multifaceted Concept of Cognitive Security (Elsevier, 2025) maps cognitive attack surfaces: attention, belief formation, narrative provenance, and transparent correction options.

Why it matters. Unveiling the Multifaceted Concept matters in the **Cognitive Security and Influence Resilience** lane because information-integrity analysis and resilience education evidence must stay separate from judgment; treating resilience labels as permission to skip provenance review is a common failure.

Source support. Unveiling the Multifaceted Concept of Cognitive Security (Elsevier, 2025) rests on [165, 2026] and [167, 2026]. The lead source's own note reads: The post describes the work as a literature review that analyzes definitions, challenges, and future trends in cognitive security and proposes a redefinition based on the concept's core components. Use them for pinning down the scope of **Unveiling the Multifaceted Concept of Cognitive Security (Elsevier, 2025)**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Unveiling the Multifaceted Concept**, reason from the sources cited in this row. [165, 2026] We provide a comprehensive review of the current state of cognitive security. [167, 2026] A LinkedIn post by Fran Casino announcing a research article titled 'Unveiling the multifaceted concept of cognitive security: Trends, perspectives, and future challenges,' published in the Elsevier journal Technology in Society. The post describes the work as a literature review that analyzes definitions, challenges, and future trends in cognitive security and proposes a redefinition based on the concept's core components. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Unveiling the Multifaceted Concept**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Unveiling the Multifaceted Concept of**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Unveiling the Multifaceted Concept** work as an **epistemic-integrity review packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Unveiling the Multifaceted Concept**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Transfer **Unveiling the Multifaceted Concept** from this module to a second motif by preserving information-integrity analysis and resilience education, replacing action with audit, and naming the blocked use.

52.2.2.6 Lesson 6: Neurocognitive resilience research literacy

Concept. Neurocognitive resilience research literacy maps cognitive attack surfaces: attention, belief formation, narrative provenance, and transparent correction options.

Why it matters. Analysts use **Neurocognitive resilience research literacy** to separate analysis of influence from persuasion design. A defensible treatment names the judgment it enables for information-integrity analysis and resilience education review, the proof limit that treating resilience labels as permission to skip provenance review would otherwise hide, and the reviewer accountable for challenge.

Source support. Neurocognitive resilience research literacy rests on [095, 2026]. The most specific cited work observes: This policy paper examines the emergence of cognitive security. Use it for the claim that **Neurocognitive resilience research literacy** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Neurocognitive resilience research literacy**, work from the cited evidence behind this row. [095, 2026] This policy paper examines the emergence of cognitive security. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. Build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Neurocognitive resilience research literacy**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape this subject work as an **epistemic-integrity review packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Neurocognitive resilience research literacy**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Apply this module's safe boundary for **Neurocognitive resilience research literacy** to another artifact while keeping information-integrity analysis and resilience education and reviewer ownership explicit.

52.2.2.7 Lesson 7: AI Development Should Prioritize Cognitive: Neurocognitive resilience research literacy Concept. AI Development Should Prioritize Cognitive: Neurocognitive resilience research literacy maps cognitive attack surfaces: attention, belief formation, narrative provenance, and transparent correction options.

Why it matters. AI Development Should Prioritize Cognitive connects classroom vocabulary to Cognitive Security and Influence Resilience practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. AI Development Should Prioritize Cognitive: Neurocognitive resilience research literacy rests on [096, 2026]. Its anchor reference records: A position paper (Stanford authors, ICLR 2026 workshop) arguing that AI research and development should prioritize cognitive security, defined as protecting human cognitive processes from hazardous influence. Use it for the working definition that **AI Development Should Prioritize Cognitive: Neurocognitive resilience research literacy** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Ground **AI Development Should Prioritize Cognitive** in the evidence the row cites. [096, 2026] A position paper (Stanford authors, ICLR 2026 workshop) arguing that AI research and development should prioritize cognitive security, defined as protecting human cognitive processes from hazardous influence. It notes that generative AI systems increasingly designed to influence beliefs and behavior raise acute governance concerns, while research on these effects remains fragmented. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **AI Development Should Prioritize Cognitive**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **AI Development Should Prioritize Cognitive**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **AI Development Should Prioritize Cognitive** work as an **epistemic-integrity review packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **AI Development Should Prioritize Cognitive**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Apply this module's safe boundary for **AI Development Should Prioritize Cognitive** to another artifact while keeping information-integrity analysis and resilience education and reviewer ownership explicit.

52.2.2.8 Lesson 8: DARPA cognitive-security research literacy Concept. DARPA cognitive-security research literacy maps cognitive attack surfaces: attention, belief formation, narrative provenance, and transparent correction options.

Why it matters. Analysts use **DARPA cognitive-security research literacy** to separate analysis of influence from persuasion design. A defensible treatment names the judgment it enables for information-integrity analysis and resilience education review, the proof limit that treating resilience labels as permission to skip provenance review would otherwise hide, and the reviewer accountable for challenge.

Source support. DARPA cognitive-security research literacy rests on [168, 2026], [169, 2026], and [170, 2026]. The lead source's own note reads: A HigherGov listing for the DARPA Intrinsic Cognitive Security (ICS) research solicitation, which seeks to develop tactical mixed-reality systems that protect users against cognitive attacks using formal methods with cognitive safeguards. Use them for pinning down the scope of **DARPA cognitive-security research literacy**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **DARPA cognitive-security research literacy**, reason from the sources cited in this row. [168, 2026] A Potomac Officers Club news article reporting on a DARPA request for proposals under its Intrinsic Cognitive Security program. The program seeks to protect mixed reality devices from cognitive attacks using mathematical approaches called formal methods, addressing risks such as flooding a device with information to induce motion sickness, distraction, or false alarms. [169, 2026] This is an official DARPA program page for the Intrinsic Cognitive Security (ICS) program, which addresses vulnerabilities in mixed reality systems that could be exploited through cognitive attacks. The program aims to develop formal mathematical methods that guarantee mixed reality designs can protect users against adversarial interference. [170, 2026] A HigherGov listing for the DARPA Intrinsic Cognitive Security (ICS) research solicitation, which seeks to develop tactical mixed-reality systems that protect users against cognitive attacks using formal methods with cognitive safeguards. The program is structured as a 36-month effort in two 18-month phases, with defined funding ranges for a mixed-reality cognition technical area and an evaluation technical area. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. Build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **DARPA cognitive-security research literacy**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape this subject work as an **epistemic-integrity review packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **DARPA cognitive-security research literacy**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **DARPA cognitive-security research literacy** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

52.2.2.9 Lesson 9: Financial due-diligence typology exercise using synthetic records and compliance boundaries Concept. Financial due-diligence typology exercise using synthetic records and compliance boundaries structures financial-pattern review as typology-driven due diligence with escalation thresholds, not proof of wrongdoing.

Why it matters. Financial due-diligence typology exercise connects classroom vocabulary to Cognitive Security and Influence Resilience practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Financial due-diligence typology exercise using synthetic records and compliance boundaries rests on [171, 2026]. The closest source to this row notes: DARPA is putting together the Intrinsic Cognitive Security (ICS) research program "to build. Use it for pinning down the scope of **Financial due-diligence typology exercise using synthetic records and compliance boundaries**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Ground **Financial due-diligence typology exercise** in the evidence the row cites. [171, 2026] DARPA is putting together the Intrinsic Cognitive Security (ICS) research program "to build. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Financial due-diligence typology exercise**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must note the typology descriptor, the bounded claim about **Financial due-diligence typology exercise using**, the intent caveat, the uncertainty threshold, the no-accusation boundary, and the reviewer who owns escalation. Shape **Financial due-diligence typology exercise** work as an **epistemic-integrity review packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Financial due-diligence typology exercise**: that a typology or pattern match is proof of intent rather than a flag requiring corroboration and alternative explanations.

Transfer task. Apply this module's safe boundary for **Financial due-diligence typology exercise** to another artifact while keeping information-integrity analysis and resilience education and reviewer ownership explicit.

52.2.2.10 Lesson 10: Formal Methods for Cognitive Guarantees in MR Systems

Concept. Formal Methods for Cognitive Guarantees in MR Systems evaluates formal guarantees as design claims requiring assumptions, limits, and independent review.

Why it matters. Formal Methods matters in the **Cognitive Security and Influence Resilience** lane because information-integrity analysis and resilience education evidence must stay separate from judgment; treating resilience labels as permission to skip provenance review is a common failure.

Source support. Formal Methods for Cognitive Guarantees in MR Systems rests on [169, 2026]. Its anchor reference records: The program aims to develop formal mathematical methods that guarantee mixed reality designs can protect users against adversarial interference. Use it for fixing what **Formal Methods for Cognitive Guarantees in MR Systems** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Formal Methods**, reason from the sources cited in this row. [169, 2026] This is an official DARPA program page for the Intrinsic Cognitive Security (ICS) program, which addresses vulnerabilities in mixed reality systems that could be exploited through cognitive attacks. The program aims to develop formal mathematical methods that guarantee mixed reality designs can protect users against adversarial interference. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Formal Methods**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Formal Methods for Cognitive Guarantees**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Formal Methods** work as an **epistemic-integrity review packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Formal Methods**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Transfer **Formal Methods** from this module to a second motif by preserving information-integrity analysis and resilience education, replacing action with audit, and naming the blocked use.

52.2.2.11 Lesson 11: Behavioral Outcomes of Human Cognitive Security (arXiv, March 2026)

Concept. Behavioral Outcomes of Human Cognitive Security (arXiv, March 2026) maps cognitive attack surfaces: attention, belief formation, narrative provenance, and transparent correction options.

Why it matters. Analysts use **Behavioral Outcomes** to separate analysis of influence from persuasion design. A defensible treatment names the judgment it enables for information-integrity analysis and resilience education review, the proof limit that treating resilience labels as permission to skip provenance review would otherwise hide, and the reviewer accountable for challenge.

Source support. Behavioral Outcomes of Human Cognitive Security (arXiv, March 2026) rests on [107, 2026]. The closest source to this row notes: It synthesizes Bayesian belief-updating with Prospect Theory to model how cognitive resources and emotional valuation shape behavior, and identifies three observable outcomes: veracity discernment, task-oriented actions, and information sharing. Use it for the claim that **Behavioral Outcomes of Human Cognitive Security (arXiv, March 2026)** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Read **Behavioral Outcomes** against the works cited for this row. [107, 2026] An arXiv research paper (March 2026) proposing an integrative modeling framework for human cognitive security, defined as the degree to which people rely on truthful information to make truth-aligned judgments. It synthesizes Bayesian belief-updating with Prospect Theory to model how cognitive resources and emotional valuation shape behavior, and identifies three observable outcomes: veracity discernment, task-oriented actions, and information sharing. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Behavioral Outcomes**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Behavioral Outcomes of Human Cognitive**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Behavioral Outcomes** work as an **epistemic-integrity review packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Behavioral Outcomes**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Transfer **Behavioral Outcomes** from this module to a second motif by preserving information-integrity analysis and resilience education, replacing action with audit, and naming the blocked use.

52.2.2.12 Lesson 12: Defining Comprehensive Cognitive Security in the Digital Era (SSRN 2024)

Concept. Defining Comprehensive Cognitive Security in the Digital Era (SSRN 2024) maps cognitive attack surfaces: attention, belief formation, narrative provenance, and transparent correction options.

Why it matters. Without explicit treatment of **Defining Comprehensive Cognitive Security**, treating resilience labels as permission to skip provenance review undermines information-integrity analysis and resilience education review; the lesson builds the habit to separate analysis of influence from persuasion design.

Source support. Defining Comprehensive Cognitive Security in the Digital Era (SSRN 2024) rests on [166, 2026]. The lead source's own note reads: Cognitive security, as an emerging field. Use it for fixing what **Defining Comprehensive Cognitive Security in the Digital Era (SSRN 2024)** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Defining Comprehensive Cognitive Security**, work from the cited evidence behind this row. [166, 2026] Cognitive security, as an emerging field. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Defining Comprehensive Cognitive Security**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Defining Comprehensive Cognitive Security in**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Defining Comprehensive Cognitive Security** work as an **epistemic-integrity review packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Defining Comprehensive Cognitive Security**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **Defining Comprehensive Cognitive Security** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

52.2.2.13 Lesson 13: Ethics of Cognitive Security (YorkSpace Dissertation) Concept. Ethics of Cognitive Security (YorkSpace Dissertation) maps cognitive attack surfaces: attention, belief formation, narrative provenance, and transparent correction options.

Why it matters. Ethics of Cognitive Security (YorkSpace Dissertation) connects classroom vocabulary to Cognitive Security and Influence Resilience practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Ethics of Cognitive Security (YorkSpace Dissertation) rests on [172, 2026]. The closest source to this row notes: This 2023 York University doctoral dissertation by Andrew Ward Buzzell provides an ethical and epistemic assessment of state power exercised to defend against information threats, a domain the author terms cognitive security. Use it for the claim that **Ethics of Cognitive Security (YorkSpace Dissertation)** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Ethics of Cognitive Security (YorkSpace Dissertation)**, work from the cited evidence behind this row. [172, 2026] This 2023 York University doctoral dissertation by Andrew Ward Buzzell provides an ethical and epistemic assessment of state power exercised to defend against information threats, a domain the author terms cognitive security. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Ethics of Cognitive Security (YorkSpace Dissertation)**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Ethics of Cognitive Security**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape this subject work as an **epistemic-integrity review packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Ethics of Cognitive Security (YorkSpace Dissertation)**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Apply this module's safe boundary for **Ethics of Cognitive Security (YorkSpace Dissertation)** to another artifact while keeping information-integrity analysis and resilience education and reviewer ownership explicit.

52.2.2.14 Lesson 14: Epistemic security and knowledge-integrity Concept. Epistemic security and knowledge-integrity protects knowledge production with provenance, dissent channels, and transparent correction—not narrative control.

Why it matters. Without explicit treatment of **Epistemic security**, treating resilience labels as permission to skip provenance review undermines information-integrity analysis and resilience education review; the lesson builds the habit to separate analysis of influence from persuasion design.

Source support. Epistemic security and knowledge-integrity rests on [307, 2026], [305, 2026], and [304, 2026]. The lead source's own note reads: NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Use them for the working definition that **Epistemic security and knowledge-integrity** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Ground **Epistemic security** in the evidence the row cites. [307, 2026] Official CISA Industrial Control Systems recommended practices page for defensive ICS/OT safety, resilience, and incident-preparation guidance. [305, 2026] Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. Build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Epistemic security**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape this subject work as an **epistemic-integrity review packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Epistemic security**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Transfer **Epistemic security** from this module to a second motif by preserving information-integrity analysis and resilience education, replacing action with audit, and naming the blocked use.

52.2.2.15 Lesson 15: Seger: Epistemic security and knowledge-integrity Concept. Seger: Epistemic security and knowledge-integrity protects knowledge production with provenance, dissent channels, and transparent correction—not narrative control.

Why it matters. Seger: Epistemic security and knowledge-integrity connects classroom vocabulary to Cognitive Security and Influence Resilience practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Seger: Epistemic security and knowledge-integrity rests on [173, 2026]. The lead source's own note reads: A project page from AI governance and ethics researcher Elizabeth Seger introducing the concept of epistemic security: protecting the processes through which information is created, distributed, and consumed in society. Use it for pinning down the scope of **Seger: Epistemic security and knowledge-integrity**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Seger: Epistemic security and knowledge-integrity**, work from the cited evidence behind this row. [173, 2026] A project page from AI governance and ethics researcher Elizabeth Seger introducing the concept of epistemic security: protecting the processes through which information is created, distributed, and consumed in society. It discusses information threats to democracies such as disinformation, eroding trust in institutions, polarization, and the misuse of generative AI, and how technologies shape knowledge production. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Seger**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Seger**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Seger: Epistemic security and knowledge-integrity** work as an **epistemic-integrity review packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Seger: Epistemic security and knowledge-integrity**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Transfer **Seger: Epistemic security and knowledge-integrity** from this module to a second motif by preserving information-integrity analysis and resilience education, replacing action with audit, and naming the blocked use.

52.2.2.16 Lesson 16: Epistemic Security: Epistemic security and knowledge-integrity Concept. Epistemic Security: Epistemic security and knowledge-integrity shows how package provenance, social trust, build integrity, and assurance controls turn a software incident into reviewable evidence.

Why it matters. Analysts use **Epistemic Security** to separate analysis of influence from persuasion design. A defensible treatment names the judgment it enables for information-integrity analysis and resilience education review, the proof limit that treating resilience labels as permission to

skip provenance review would otherwise hide, and the reviewer accountable for challenge.

Source support. Epistemic Security: Epistemic security and knowledge-integrity rests on [174, 2026]. The closest source to this row notes: A February 2025 Demos report by Elizabeth Seger, Hannah Perry, and Jamie Hancock on strengthening the UK's information supply chain. Use it for pinning down the scope of **Epistemic Security: Epistemic security and knowledge-integrity**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Ground **Epistemic Security** in the evidence the row cites. [174, 2026] A February 2025 Demos report by Elizabeth Seger, Hannah Perry, and Jamie Hancock on strengthening the UK's information supply chain. It frames epistemic security, securing healthy and robust flows of trustworthy information, as essential to countering what it calls a democratic emergency driven by institutional distrust, the decline of local news, and concentrated control of information by social media platforms. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Epistemic Security**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Epistemic Security**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Epistemic Security** work as an **epistemic-integrity review packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Epistemic Security**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Apply this module's safe boundary for **Epistemic Security** to another artifact while keeping information-integrity analysis and resilience education and reviewer ownership explicit.

52.2.2.17 Lesson 17: Tackling Threats to Informed Decision-Making (Turing Institute) Concept. Tackling Threats to Informed Decision-Making (Turing Institute)

Tackling Threats to Informed Decision-Making (Turing Institute) focuses on transparent resilience education: provenance, audience harm, attribution caution, and non-manipulative response options.

Why it matters. Tackling Threats connects classroom vocabulary to Cognitive Security and Influence Resilience practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Tackling Threats to Informed Decision-Making (Turing Institute) rests on [175, 2026]. The most specific cited work observes: It examines threats to informed decision-making and collective action, analyzing vulnerabilities in social epistemic infrastructures such as adversaries and blunderers, attention scarcity, group polarization, and the erosion of trust. Use it for the claim that **Tackling Threats to Informed Decision-Making (Turing Institute)** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Read **Tackling Threats** against the works cited for this row. [175, 2026] A 2020 Alan Turing Institute report, authored by Elizabeth Seger, Shahar Avin, and colleagues from Cambridge and the UK Defence Science and Technology Laboratory, on promoting epistemic security in technologically advanced democracies. It examines threats to informed decision-making and collective action, analyzing vulnerabilities in social epistemic infrastructures such as adversaries and blunderers, attention scarcity, group polarization, and the erosion of trust. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Tackling Threats**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Tackling Threats to Informed Decision-Making**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Tackling Threats** work as an **epistemic-integrity review packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Tackling Threats**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Apply this module's safe boundary for **Tackling Threats** to another artifact while keeping information-integrity analysis and resilience education and reviewer ownership explicit.

52.2.2.18 Lesson 18: Epistemic Governance in Crisis: Epistemic security and knowledge-integrity Concept. Epistemic Governance in Crisis: Epistemic security and knowledge-integrity

Epistemic Governance in Crisis: Epistemic security and knowledge-integrity protects knowledge production with provenance, dissent channels, and transparent correction—not narrative control.

Why it matters. Analysts use **Epistemic Governance in Crisis** to separate analysis of influence from persuasion design. A defensible treatment names the judgment it enables for information-integrity analysis and resilience education review, the proof limit that treating resilience labels as permission to skip provenance review would otherwise hide, and the reviewer accountable for challenge.

Source support. Epistemic Governance in Crisis: Epistemic security and knowledge-integrity rests on [001, 2026]. Its anchor reference records: This article examines the concept of epistemic governance during crises. Use it for the working definition that **Epistemic Governance in Crisis: Epistemic security and knowledge-integrity** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Epistemic Governance in Crisis**, work from the cited evidence behind this row. [001, 2026] This article examines the concept of epistemic governance during crises. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Epistemic Governance in Crisis**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Epistemic Governance in Crisis**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Epistemic Governance in Crisis** work as an **epistemic-integrity review packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Epistemic Governance in Crisis**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **Epistemic Governance in Crisis** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

52.2.3 Cognitive Security: Foundations and Definitions worked safe example: synthetic inputs, evidence, and review

Worked example: a sample public-library class evaluates a synthetic rumor about a community service and compares transparent correction options. [238, 2026]; [239, 2026].

Triangulation anchors. In module 37's worked-example section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **cognitive resilience and epistemic integrity**. Learners use a **epistemic-integrity review packet** and keep this boundary visible: No manipulation, covert persuasion, medicalized claims, or population-level targeting.

Frame. The classroom question centers on **Cognitive security definitions and scope**. Excluded actions stay explicit, and the **Cognitive-Resilience Lens** planning question is: How does the module protect autonomy, attention, trust, and decision quality without designing persuasion?

Inputs. For the **Cognitive security definitions and scope** scenario, use sample posts, source timestamps, public-service facts, and a media-literacy rubric. The Cognitive-Resilience Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Cognitive security definitions and scope**, students trace narrative provenance, separate observation from attribution, name audience harms, and design a transparent lesson. Pause whenever an inference about Cognitive security definitions and scope appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Cognitive security definitions and scope** classroom scenario; unit artifact = epistemic-integrity review packet; evidence = allowed inputs; method = information-integrity analysis and resilience education; output = a narrative-risk map with caveats, response options, and no microtargeted persuasion; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Cognitive security definitions and scope** as "Cognitive-Resilience Lens confirms it" is not enough. The revision ties the claim to information-integrity analysis and resilience education, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Cognitive security definitions and scope** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

52.2.4 Cognitive Security: Foundations and Definitions practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Cognitive-Resilience Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**.

Triangulation anchors. In module 37's practice-sequence section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Cognitive security definitions and scope, Comprehensive Definition: State and Process Against Malign Influence, Cognitive Security vs. Cybersecurity vs. Information Security; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Cognitive Security and Influence Resilience** lane.
2. Frame	Answer the lens question: How does the module protect autonomy, attention, trust, and decision quality without designing persuasion?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Cognitive security definitions and scope: narrative-risk map with provenance, uncertainty, audience harms, and response options.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the epistemic-integrity review packet fields for Cognitive security definitions and scope.	Unit profile note.	Evidence artifacts include provenance chain, correction option.
4. Challenge	Test the misconception that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.	Failure-mode note.	The artifact applies the key distinction: separate analysis of influence from persuasion design.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

52.2.4.1 Cognitive Security: Foundations and Definitions instructor notes: source reasoning, review points, and studio focus

Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**. [238, 2026]; [239, 2026].

52.2.4.2 Cognitive Security: Foundations and Definitions extension exercise: peer validation and refresh trigger review

Evidence anchor. Section 52; [238, 2026].

Have learners swap artifacts and apply the **Cognitive-Resilience Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**.

52.2.5 Cognitive Security: Foundations and Definitions knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 52; [238, 2026].

1. Explain how **Cognitive security definitions and scope** is defined here; name the source descriptor that supports the definition.
2. Contrast **Cognitive security definitions and scope** with **Comprehensive Definition: State and Process Against Malign Influence** using the **Cognitive-Resilience Lens** artifact fields.
3. Identify one failure mode from the **Cognitive Security and Influence Resilience** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which response informs people without crossing into MISO-style manipulation or unverified attribution?
5. Correct this misconception: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

52.2.5.1 Cognitive Security: Foundations and Definitions answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Cognitive security definitions and scope** without source evidence, uncertainty, or a safe transfer task.

52.3 Cognitive Security: Foundations and Definitions assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 52; [238, 2026].

52.3.1 Cognitive Security: Foundations and Definitions evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 52; [238, 2026].

52.3.2 Cognitive Security: Foundations and Definitions transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 52; [238, 2026].

52.3.2.1 Cognitive Security: Foundations and Definitions lineage and source tradition: profile, concepts, and first anchors This sits in the **Cognitive Security and Influence Resilience** lineage: protecting attention, belief formation, and decision quality without turning resilience education into manipulation. [238, 2026]; [239, 2026].

52.3.2.2 Cognitive Security: Foundations and Definitions working model: inputs, constraints, transforms, outputs, and oversight Evidence anchor. Section 52; [238, 2026].
The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**, with provenance and reviewability throughout.

52.3.2.3 Cognitive Security: Foundations and Definitions knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [238, 2026]; [239, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

52.3.2.4 Cognitive Security: Foundations and Definitions transfer contracts: authority, evidence, tools, and auditable output Evidence anchor. Section 52; [238, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**.
- **Evidence contract:** keep the **Cognitive Security and Influence Resilience** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

52.3.2.5 Cognitive Security: Foundations and Definitions profile emphasis and local focus: method stack and topic cluster Evidence anchor. Section 52; [238, 2026].
The matched profile emphasizes protecting attention, belief formation, and decision quality without turning resilience education into manipulation. The method stack is claim decomposition, narrative provenance, inoculation framing, bias checks, audience-risk review, and after-action learning; the local topic cluster is **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**.

52.3.3 Cognitive Security: Foundations and Definitions evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 52; [238, 2026].
Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Cognitive Security and Influence Resilience** profile tells reviewers what evidence is strong enough for the module artifact built around **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**.

52.3.3.1 Cognitive Security: Foundations and Definitions guide source spine: inherited keys and local citation roles Primary guide citations: [238, 2026]; [239, 2026]; [244, 2026]; [273, 2026]; [276, 2026]; [285, 2026]; [286, 2026]; [290, 2026]; [294, 2026]; [165, 2026]; [166, 2026]; [167, 2026]; [095, 2026]; [096, 2026]; [168, 2026]; [169, 2026]; [170, 2026]; [171, 2026]; [107, 2026]; [172, 2026]; [173, 2026]; [174, 2026]; [175, 2026]; [001, 2026]; [307, 2026]; [305, 2026]; [304, 2026].

52.3.3.2 Cognitive Security: Foundations and Definitions verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [238, 2026]; [239, 2026].

Tier	What counts	How it is used
Source guide	[238, 2026]; [239, 2026]; [244, 2026]; [273, 2026]; [276, 2026]; [285, 2026]; [286, 2026]; [290, 2026]; [294, 2026]; [165, 2026]; [166, 2026]; [167, 2026]; [095, 2026]; [096, 2026]; [168, 2026]; [169, 2026]; [170, 2026]; [171, 2026]; [107, 2026]; [172, 2026]; [173, 2026]; [174, 2026]; [175, 2026]; [001, 2026]; [307, 2026]; [305, 2026]; [304, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 37's source-canon section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Maintenance rule: Perplexity may suggest candidates for **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence** and [238, 2026]; [239, 2026], but only directly verified source URLs are encoded as citations.

52.3.3.3 Cognitive Security: Foundations and Definitions intelligence practice lens: evidence artifact and safety check Practice lens: **Cognitive-Resilience Lens** for **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**. [238, 2026]; [239, 2026].

Planning question: How does the module protect autonomy, attention, trust, and decision quality without designing persuasion?

Evidence artifact: narrative-risk map with provenance, uncertainty, audience harms, and response options.

Validation rule: distinguish observation, attribution, impact assessment, and resilience response. Applied to **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**.

Handoff contract: handoff supports transparency, education, and resilience, not microtargeted influence or deception.

Safety check: exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning.

52.3.3.4 Cognitive Security: Foundations and Definitions runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 52; [238, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	37.99	37.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Cognitive Security: Foundations and Definitions to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Bounded autonomy, procurement, incident-response, and assurance studio	37.101	37.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Cognitive Security: Foundations and Definitions	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Model-card, recoverability, retention, and learner-support evidence package	37.102	37.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Cognitive Security: Foundations and Definitions	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Cognitive security definitions and scope	37.1	37.1 source title transformed into safe curriculum treatment; original: What Is Cognitive Security? Definitions, Scope, Emergence	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Comprehensive Definition: State and Process Against Malign Influence	37.1.1	37.1.1 Comprehensive Definition: State and Process Against Malign Influence	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Cognitive Security vs. Cybersecurity vs. Information Security	37.1.2	37.1.2 Cognitive Security vs. Cybersecurity vs. Information Security	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Three Pillars: Awareness + Situation Awareness + Purposeful Action	37.1.3	37.1.3 Three Pillars: Awareness + Situation Awareness + Purposeful Action	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Unveiling the Multifaceted Concept of Cognitive Security (Elsevier, 2025)	37.2	37.2 Unveiling the Multifaceted Concept of Cognitive Security (Elsevier, 2025)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Neurocognitive resilience research literacy	37.3	37.3 source title transformed into safe curriculum treatment; original: Cognitive Security in the Age of AI (RESAID Policy Paper, 2025)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Neurocognitive resilience research literacy	37.4	37.4 source title transformed into safe curriculum treatment; original: AI Development Should Prioritize Cognitive Security (NeurIPS Position Paper, 2023)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
DARPA cognitive-security research literacy	37.4.1	37.4.1 source title transformed into safe curriculum treatment; original: DARPA Intrinsic Cognitive Security (ICS) Program	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Financial due-diligence typology exercise using synthetic records and compliance boundaries	37.4.2	37.4.2 source title transformed into safe curriculum treatment; original: Mixed Reality Cognitive Attack Typology	Economic-Security Due-Diligence Lens	economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary	exclude sanctions evasion, laundering methods, threshold gaming, procurement bypasses, and tailored targeting of real firms
Formal Methods for Cognitive Guarantees in MR Systems	37.4.3	37.4.3 Formal Methods for Cognitive Guarantees in MR Systems	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Behavioral Outcomes of Human Cognitive Security (arXiv, March 2026)	37.5	37.5 Behavioral Outcomes of Human Cognitive Security (arXiv, March 2026)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Defining Comprehensive Cognitive Security in the Digital Era (SSRN 2024)	37.6	37.6 Defining Comprehensive Cognitive Security in the Digital Era (SSRN 2024)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Ethics of Cognitive Security (YorkSpace Dissertation)	37.7	37.7 Ethics of Cognitive Security (YorkSpace Dissertation)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Epistemic security and knowledge-integrity	37.8	37.8 source title transformed into safe curriculum treatment; original: Epistemic Security: Protecting Knowledge Production and Distribution	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Epistemic security and knowledge-integrity	37.8.1	37.8.1 source title transformed into safe curriculum treatment; original: Seger: Epistemic Security as a Field	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Epistemic security and knowledge-integrity	37.8.2	37.8.2 source title transformed into safe curriculum treatment; original: Epistemic Security 2029: Fortifying the UK's Information Supply Chain	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Tackling Threats to Informed Decision-Making (Turing Institute)	37.8.3	37.8.3 Tackling Threats to Informed Decision-Making (Turing Institute)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Epistemic security and knowledge-integrity	37.8.4	37.8.4 source title transformed into safe curriculum treatment; original: Epistemic Governance in Crisis: A Complexity Approach	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning

52.3.3.5 Cognitive Security: Foundations and Definitions reusable subsection contract: topic rows, artifacts, and safety duties Evidence anchor. Section 52; [238, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Cognitive security definitions and scope	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Comprehensive Definition: State and Process Against Malign Influence	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Cognitive Security vs. Cybersecurity vs. Information Security	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Three Pillars: Awareness + Situation Awareness + Purposeful Action	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Unveiling the Multifaceted Concept of Cognitive Security (Elsevier, 2025)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Neurocognitive resilience research literacy	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
AI Development Should Prioritize Cognitive: Neurocognitive resilience research literacy	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
DARPA cognitive-security research literacy	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Financial due-diligence typology exercise using synthetic records and compliance boundaries	Economic-Security Due-Diligence Lens	economic-security packet with entity evidence, sanctions program, red flags, supplier context, uncertainty, and compliance boundary	exclude sanctions evasion, laundering methods, threshold gaming, procurement bypasses, and tailored targeting of real firms

Lesson topic	Practice lens	Evidence artifact	Safety check
Formal Methods for Cognitive Guarantees in MR Systems	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Behavioral Outcomes of Human Cognitive Security (arXiv, March 2026)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Defining Comprehensive Cognitive Security in the Digital Era (SSRN 2024)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Ethics of Cognitive Security (YorkSpace Dissertation)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Epistemic security and knowledge-integrity	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Seger: Epistemic security and knowledge-integrity	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Epistemic Security: Epistemic security and knowledge-integrity	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Tackling Threats to Informed Decision-Making (Turing Institute)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Epistemic Governance in Crisis: Epistemic security and knowledge-integrity	AI/Data Accountability Lens	AI/data impact card with authority, provenance, model version, impact score, register status, human owner, and review cadence	reject automated adverse action, hidden surveillance expansion, unowned outputs, unreviewed model drift, and opaque downstream reuse

52.3.3.6 Cognitive Security: Foundations and Definitions annotated source ledger: real titles and local contribution Each source cited by this **Cognitive Security and Influence Resilience** module is paired below with its real title and a one-line note on what it contributes to **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**.

Source	Cited work	What it contributes	Status
[238, 2026]	Recommendation on the Ethics of Artificial Intelligence	The official UNESCO page for the Recommendation on the Ethics of Artificial Intelligence, the first global standard-setting instrument on AI ethics, adopted in 2021 and applicable to all 194 member states. It outlines four core values, including human rights protection and environmental flourishing, and ten guiding principles such as proportionality, privacy, transparency, and fairness.	verified source-guide
[239, 2026]	Digital Space and Human Rights	Official OHCHR digital rights portal.	original source-guide
[244, 2026]	AI and Education	Official UNESCO GEM AI and education source hub.	original source-guide
[273, 2026]	WCAG 2 Overview	The W3C Web Accessibility Initiative overview of the Web Content Accessibility Guidelines (WCAG), an international standard for making web content accessible to people with disabilities. It explains that WCAG is organized around four principles (perceivable, operable, understandable, robust) with testable success criteria at three conformance levels (A, AA, AAA), and covers versions 2.0, 2.1, and 2.2.	verified source-guide

Source	Cited work	What it contributes	Status
[276, 2026]	What is a Data Protection Impact Assessment and When Is This Mandatory?	A European Data Protection Board FAQ page, part of its data protection guide for small businesses, explaining Data Protection Impact Assessments (DPIAs) and when they are mandatory. It describes a DPIA as a written assessment of the impact of a planned processing operation, required when processing poses high risks to individuals' rights.	verified source-guide
[285, 2026]	NIST AI Resource Center	The NIST AI Resource Center (AIRC), a government platform supporting implementation of the NIST AI Risk Management Framework, a voluntary framework for managing AI risk. It provides the core framework along with a playbook of practical actions, profiles tailored to specific sectors and technologies, use cases, and crosswalks linking the framework to other governance structures.	verified source-guide
[286, 2026]	Model Cards for Model Reporting	The arXiv abstract for "Model Cards for Model Reporting" (2018) by Mitchell, Wu, Zaldivar, and colleagues, which introduces a framework for transparent documentation of machine learning models. Model cards are short accompanying documents that report a model's benchmarked performance across varied conditions, including different cultural, demographic, and phenotypic groups, along with intended use, evaluation methodology, and deployment considerations.	verified source-guide
[290, 2026]	NIST SP 800-218A: Secure Software Development Practices for Generative AI and Dual-Use Foundation Models	NIST Special Publication 800-218A (July 2024), which augments the Secure Software Development Framework with practices specific to AI model development across the software lifecycle. Produced in response to Executive Order 14110, it addresses AI model producers, developers building on those models, and acquirers of AI systems, and is designed to be used alongside NIST SP 800-218.	verified source-guide
[294, 2026]	M-25-21: Accelerating Federal Use of AI through Innovation, Governance, and Public Trust	An April 2025 Office of Management and Budget memorandum (M-25-21) directing executive branch agencies on federal use of artificial intelligence. Issued under Executive Order 14179, it instructs agencies to accelerate adoption of AI to improve public services and government efficiency while maintaining safeguards for civil rights, civil liberties, and privacy.	verified source-guide
[165, 2026]	Unveiling the multifaceted concept of cognitive security	We provide a comprehensive review of the current state of cognitive security.	original source-guide
[166, 2026]	Defining comprehensive cognitive security in the digital era: Literature review and concept analysis	Cognitive security, as an emerging field.	original source-guide

Source	Cited work	What it contributes	Status
[167, 2026]	Unveiling the multifaceted concept of cognitive security	A LinkedIn post by Fran Casino announcing a research article titled 'Unveiling the multifaceted concept of cognitive security: Trends, perspectives, and future challenges,' published in the Elsevier journal Technology in Society. The post describes the work as a literature review that analyzes definitions, challenges, and future trends in cognitive security and proposes a redefinition based on the concept's core components.	verified practitioner context; secondary evidence only
[095, 2026]	COGNITIVE SECURITY IN THE AGE OF AI	This policy paper examines the emergence of cognitive security.	original source-guide
[096, 2026]	AI DEVELOPMENT SHOULD PRIORITIZE COGNITIVE SECURITY	A position paper (Stanford authors, ICLR 2026 workshop) arguing that AI research and development should prioritize cognitive security, defined as protecting human cognitive processes from hazardous influence. It notes that generative AI systems increasingly designed to influence beliefs and behavior raise acute governance concerns, while research on these effects remains fragmented.	verified source-guide
[168, 2026]	DARPA Seeks Proposals For Intrinsic Cognitive Security Program	A Potomac Officers Club news article reporting on a DARPA request for proposals under its Intrinsic Cognitive Security program. The program seeks to protect mixed reality devices from cognitive attacks using mathematical approaches called formal methods, addressing risks such as flooding a device with information to induce motion sickness, distraction, or false alarms.	verified source-guide
[169, 2026]	ICS / DARPA	This is an official DARPA program page for the Intrinsic Cognitive Security (ICS) program, which addresses vulnerabilities in mixed reality systems that could be exploited through cognitive attacks. The program aims to develop formal mathematical methods that guarantee mixed reality designs can protect users against adversarial interference.	verified source-guide
[170, 2026]	Intrinsic Cognitive Security (ICS) - HigherGov	A HigherGov listing for the DARPA Intrinsic Cognitive Security (ICS) research solicitation, which seeks to develop tactical mixed-reality systems that protect users against cognitive attacks using formal methods with cognitive safeguards. The program is structured as a 36-month effort in two 18-month phases, with defined funding ranges for a mixed-reality cognition technical area and an evaluation technical area.	verified source-guide
[171, 2026]	DARPA Preps Program to Protect Mixed Reality Users	DARPA is putting together the Intrinsic Cognitive Security (ICS) research program "to build.	original source-guide

Source	Cited work	What it contributes	Status
[107, 2026]	Behavioral Outcomes of Human Cognitive Security	An arXiv research paper (March 2026) proposing an integrative modeling framework for human cognitive security, defined as the degree to which people rely on truthful information to make truth-aligned judgments. It synthesizes Bayesian belief-updating with Prospect Theory to model how cognitive resources and emotional valuation shape behavior, and identifies three observable outcomes: veracity discernment, task-oriented actions, and information sharing.	verified source-guide
[172, 2026]	The Ethics of Cognitive Security - YorkSpace	This 2023 York University doctoral dissertation by Andrew Ward Buzzell provides an ethical and epistemic assessment of state power exercised to defend against information threats, a domain the author terms cognitive security.	verified source-guide
[173, 2026]	Epistemic Security - Elizabeth Seger	A project page from AI governance and ethics researcher Elizabeth Seger introducing the concept of epistemic security: protecting the processes through which information is created, distributed, and consumed in society. It discusses information threats to democracies such as disinformation, eroding trust in institutions, polarization, and the misuse of generative AI, and how technologies shape knowledge production.	verified source-guide
[174, 2026]	Epistemic Security 2029: Fortifying the UK's Information Supply	A February 2025 Demos report by Elizabeth Seger, Hannah Perry, and Jamie Hancock on strengthening the UK's information supply chain. It frames epistemic security, securing healthy and robust flows of trustworthy information, as essential to countering what it calls a democratic emergency driven by institutional distrust, the decline of local news, and concentrated control of information by social media platforms.	verified source-guide
[175, 2026]	Tackling threats to informed decision- making in democratic societies	A 2020 Alan Turing Institute report, authored by Elizabeth Seger, Shahar Avin, and colleagues from Cambridge and the UK Defence Science and Technology Laboratory, on promoting epistemic security in technologically advanced democracies. It examines threats to informed decision-making and collective action, analyzing vulnerabilities in social epistemic infrastructures such as adversaries and blunderers, attention scarcity, group polarization, and the erosion of trust.	verified source-guide
[001, 2026]	Epistemic Governance in the Context of Crisis	This article examines the concept of epistemic governance during crises.	original source-guide
[307, 2026]	ICS Recommended Practices	Official CISA Industrial Control Systems recommended practices page for defensive ICS/OT safety, resilience, and incident-preparation guidance.	original source-guide
[305, 2026]	DevSecOps	Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support.	original source-guide

Source	Cited work	What it contributes	Status
[304, 2026]	Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities	NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences.	verified source-guide

Where this sits. This module's overview is Section 52; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

52.3.4 Cognitive Security: Foundations and Definitions governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 52; [238, 2026].

52.3.5 Cognitive Security: Foundations and Definitions analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 37's governance-boundary section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **Cognitive Security and Influence Resilience** for **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**. [238, 2026]; [239, 2026].

Curriculum topic spine: Cognitive security definitions and scope, **Comprehensive Definition: State and Process Against Malign Influence**, **Cognitive Security vs. Cybersecurity vs. Information Security**. **Verified anchor cluster:** [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]; [OECD, 2026c]; [for Security Policy, 2025]; [Community, 2020a].

Conceptual depth: protecting attention, belief formation, and decision quality without turning resilience education into manipulation.

Method stack: claim decomposition, narrative provenance, inoculation framing, bias checks, audience-risk review, and after-action learning.

Composability contract: separate descriptive analysis, normative assessment, response options, and protected-audience considerations.

Known failure modes: counter-messaging as manipulation, overclaiming intent, pathologizing audiences, and collapsing uncertainty into moral certainty.

Defensive boundary: practice uses benign simulations and resilience education; it does not create persuasion campaigns, impersonation, or deception plans. Applied to **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**.

Anchor	Why it matters here
[Cybersecurity and Agency, 2024b]	Official CISA guidance on foreign influence operations targeting critical infrastructure. Checked as of 2026-05-21; role: source_quality_anchor.
[Organization, 2026b]	Official NATO counter-information-threat guidance. Checked as of 2026-05-21; role: source_quality_anchor.
[Cybersecurity and Agency, 2026b]	Official CISA election-security source for public-resilience, foreign-influence awareness, rumor control, and defensive communication framing. Checked as of 2026-05-21; role: curriculum_anchor.
[Organization, 2026c]	Official NATO source for hybrid-threat resilience across cyber, information, economic, political, and military pressure. Checked as of 2026-05-21; role: curriculum_anchor.
[OECD, 2026c]	Official OECD policy source for information integrity, governance responses, public trust, and democratic resilience. Checked as of 2026-05-21; role: curriculum_anchor.
[for Security Policy, 2025]	Policy-scholarship source for cognitive security, information literacy, critical thinking, and whole-of-society resilience. Checked as of 2026-05-21; role: curriculum_anchor.
[Community, 2020a]	Official IC framework for AI goals, authorities, human judgment, bias mitigation, testing, documentation, explainability, and review. Checked as of 2026-05-21; role: curriculum_anchor.

52.3.5.1 Cognitive Security: Foundations and Definitions evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **Cognitive Security and Influence Resilience** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [238, 2026]; [239, 2026].

52.3.6 Cognitive Security: Foundations and Definitions agentic boundary: assist, approve, block, and record

Evidence anchor. Section 52; [238, 2026].

AGEINT translation is bounded by the **Cognitive Security and Influence Resilience** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**.

52.3.6.1 Cognitive Security: Foundations and Definitions permitted defensive utility: curriculum uses and safe outputs

Evidence anchor. Section 52; [238, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**.

52.3.6.2 Cognitive Security: Foundations and Definitions excluded operational boundary: blocked actions and stop rules

Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [238, 2026]; [239, 2026] and **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

52.3.7 Cognitive Security: Foundations and Definitions governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 52; [238, 2026].

Governance is practiced as a gate on the **Cognitive Security and Influence Resilience** lane. Learners use the **Cognitive-Resilience Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**.

52.3.7.1 Cognitive Security: Foundations and Definitions governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [238, 2026]; [239, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Cognitive Security and Influence Resilience** failure modes and the **Cognitive-Resilience Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

52.3.7.2 Cognitive Security: Foundations and Definitions evidence package handoff: appendices, records, and reuse **Evidence anchor.** Section 52; [238, 2026].
Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Cognitive-Resilience Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**.

52.3.7.3 Cognitive Security: Foundations and Definitions current-source assurance: verified anchors and local artifact fit The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**. [238, 2026]; [239, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_cisa_foreign_influence` for **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**?	Preparing for and Mitigating Foreign Influence Operations; lane `source_quality_spine`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official CISA guidance on foreign influence operations targeting critical infrastructure.
What does the module inherit from `official_nato_counter_information_threats` for **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**?	Countering Information Threats; lane `source_quality_spine`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official NATO counter-information-threat guidance.
What does the module inherit from `official_cisa_election_security_influence` for **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**?	Election Security; lane `cognitive_influence_security`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official CISA election-security source for public-resilience, foreign-influence awareness, rumor control, and defensive communication framing.
What does the module inherit from `official_nato_hybrid_threats` for **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**?	Countering Hybrid Threats; lane `cognitive_influence_security`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official NATO source for hybrid-threat resilience across cyber, information, economic, political, and military pressure.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 52; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

52.3.8 Cognitive Security: Foundations and Definitions assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 52; [238, 2026].

52.3.9 Cognitive Security: Foundations and Definitions assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 52; [238, 2026].

52.3.9.1 Cognitive Security: Foundations and Definitions capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence** and [238, 2026]; [239, 2026].

52.3.9.2 Cognitive Security: Foundations and Definitions instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence** and [238, 2026]; [239, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

52.3.9.3 Cognitive Security: Foundations and Definitions assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Cognitive security definitions and scope	Completed **narrative-risk map with provenance, uncertainty, audience harms, and response options** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Comprehensive Definition: State and Process Against Malign Influence	Completed **narrative-risk map with provenance, uncertainty, audience harms, and response options** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Cognitive Security vs. Cybersecurity vs. Information Security	Completed **narrative-risk map with provenance, uncertainty, audience harms, and response options** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

52.3.10 Cognitive Security: Foundations and Definitions refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [238, 2026]; [239, 2026] and **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**.

52.3.10.1 Cognitive Security: Foundations and Definitions refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**. The local signals begin with [238, 2026]; [239, 2026].

52.3.10.2 Cognitive Security: Foundations and Definitions claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**, and the source spine for these checks begins with [238, 2026]; [239, 2026].

52.3.11 Cognitive Security: Foundations and Definitions reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [238, 2026]; [239, 2026].

Triangulation anchors. In module 37's review-checklist section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence**. [238, 2026]; [239, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

52.3.12 Cognitive Security: Foundations and Definitions learning-path links: module map, overview, and curriculum atlas

Use the cross-links below to place **Cognitive security definitions and scope; Comprehensive Definition: State and Process Against Malign Influence** in the wider unit: the orientation sets the frame, the parent unit supplies the shared safety posture, and the neighbouring modules show what evidence enters and leaves. Lead sources: [238, 2026]; [239, 2026].

Section 2, Section 51, Section 53

53 Neurocognitive Mechanisms of Cognitive Security

53.0.1 Neurocognitive Mechanisms of Cognitive Security figures and course links: visual evidence, source flow, and navigation

The module uses Figure 112 and Figure 107 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 51, Section 52, Section 54.
This module teaches the **Cognitive Security and Influence Resilience** lane through a bounded, source-backed coursebook chapter. [238, 2026]; [240, 2026].

53.1 Cognitive Security and Influence Resilience frame for Neurocognitive Mechanisms of Cognitive Security: source context, topic focus, and reader task

Evidence anchor. Section 53; [238, 2026].

53.1.1 Neurocognitive Mechanisms of Cognitive Security orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 53; [238, 2026].

53.1.2 Neurocognitive Mechanisms of Cognitive Security conceptual primer: source context, core model, and reader task

This chapter teaches cognitive security as protection of attention, trust, memory, and decision quality without creating manipulation. The chapter uses **Cognitive-Resilience Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats**.
The central distinction is to separate analysis of influence from persuasion design. Core topics include **Understanding Neurocognitive Mechanisms of Cognitive Security (Neuroscience & Biobehavioral Reviews, 2025); Executive Brain Systems and Vulnerability to Information Threats; Affective Systems: Emotional Exploitation in Manipulation**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [238, 2026]; [240, 2026].
Learners move from vocabulary and the **Cognitive-Resilience Lens** distinction through topic lessons on **Understanding Neurocognitive Mechanisms of Cognitive Security (Neuroscience & Biobehavioral Reviews, 2025)** with evidence and misconception checks, then assemble a **narrative-risk map with provenance, uncertainty, audience harms, and response options** with safety and rights gates.

53.1.3 Neurocognitive Mechanisms of Cognitive Security learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 53; [238, 2026].

- Connect **Understanding Neurocognitive Mechanisms of Cognitive Security (Neuroscience & Biobehavioral Reviews, 2025) and Executive Brain Systems and Vulnerability to Information Threats** to **Cognitive Security and Influence Resilience** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate analysis of influence from persuasion design; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as counter-messaging as manipulation, overclaiming intent, pathologizing audiences, and collapsing uncertainty into moral certainty, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: practice uses benign simulations and resilience education; it does not create persuasion campaigns, impersonation, or deception plans.

53.1.4 Neurocognitive Mechanisms of Cognitive Security core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 53; [238, 2026].

Term	Working definition
Narrative provenance	where a claim, frame, or story came from and how it spread
Prebunking	transparent education that helps people recognize misleading patterns before exposure
Audience harm	a privacy, dignity, autonomy, or trust risk for people receiving information
Attribution caution	the rule that intent and origin claims need strong evidence
Resilience response	a transparent education, correction, or process improvement that avoids manipulation
MISO boundary	the line between accountable public messaging analysis and covert influence design
Inoculation	building recognition of manipulation tactics without deploying persuasion against a population
Understanding Neurocognitive Mechanisms of…	Key terms: Understanding, Neurocognitive, Mechanisms.
Executive Brain Systems and Vulnerability to…	Key terms: Executive, Brain, Systems.

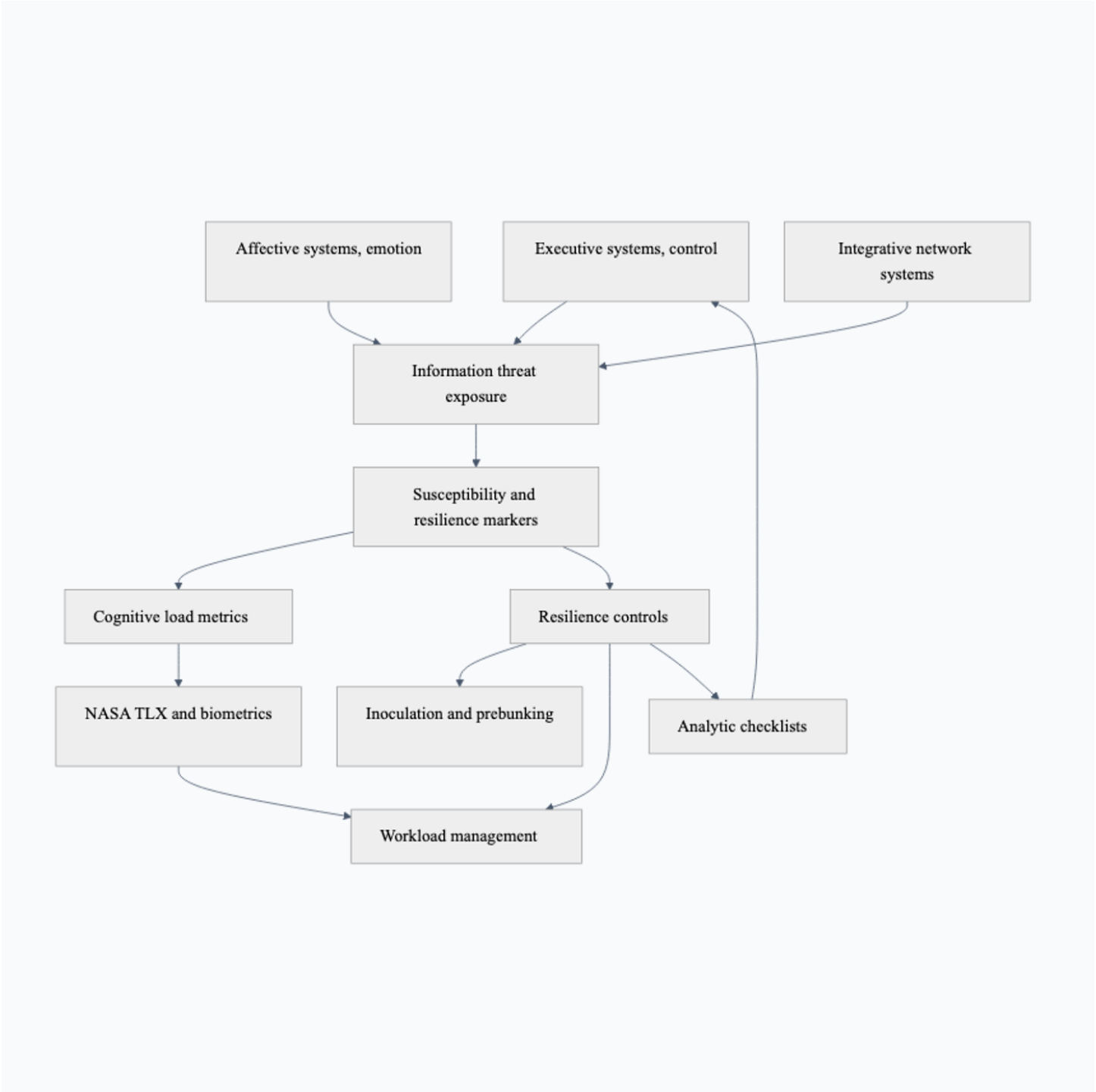


Figure 112: A defensive model linking executive, affective, and integrative brain systems to measurable susceptibility markers and the resilience controls that strengthen them. The captioned view belongs to the cognitive security / neurocognitive mechanisms of cognitive security section and should be read as a map of Executive systems, control, Information threat exposure, Affective systems, emotion, and Integrative network systems, not as a capability score or live-task instruction.

53.2 Cognitive-Resilience Lens path for Neurocognitive Mechanisms of Cognitive Security: lesson cluster, safe artifact, and review

Evidence anchor. Section 53; [238, 2026].

53.2.1 Neurocognitive Mechanisms of Cognitive Security practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 53; [238, 2026].

53.2.2 Neurocognitive Mechanisms of Cognitive Security topic lessons: source-backed concepts and transfer tasks

This module builds cognitive security as protection of attention, trust, memory, and decision quality without creating manipulation. The sequence opens with **Understanding Neurocognitive Mechanisms of Cognitive Security (Neuroscience & Biobehavioral Reviews, 2025)**, **Executive Brain Systems and Vulnerability to Information Threats**, **Affective Systems: Emotional Exploitation in Manipulation** and applies the **Cognitive-Resilience Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 107; module overview Section 53; curriculum atlas Section 2.

Triangulation anchors. In module 38's topic-lessons section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

53.2.2.1 Lesson 1: Understanding Neurocognitive Mechanisms of Cognitive Security (Neuroscience & Biobehavioral Reviews, 2025) Concept. Understanding Neurocognitive Mechanisms of Cognitive Security (Neuroscience & Biobehavioral Reviews, 2025) maps cognitive attack surfaces: attention, belief formation, narrative provenance, and transparent correction options.

Why it matters. Analysts use **Understanding Neurocognitive Mechanisms** to separate analysis of influence from persuasion design. A defensible treatment names the judgment it enables for information-integrity analysis and resilience education review, the proof limit that treating resilience labels as permission to skip provenance review would otherwise hide, and the reviewer accountable for challenge.

Source support. Understanding Neurocognitive Mechanisms of Cognitive Security (Neuroscience & Biobehavioral Reviews, 2025) rests on [176, 2026] and [177, 2026]. The most specific cited work observes: The authors synthesize research on why people fall victim to false or deceptive information, proposing that certain brain systems are more exploitable than others. Use them for pinning down the scope of **Understanding Neurocognitive Mechanisms of Cognitive Security (Neuroscience & Biobehavioral Reviews, 2025)**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Understanding Neurocognitive Mechanisms**, reason from the sources cited in this row. [176, 2026] Cognitive security is a relatively new field that aims to understand and defend against. [177, 2026] A peer-reviewed review article published in Neuroscience & Biobehavioral Reviews (December 2025) by Crum and colleagues examining the neurocognitive mechanisms of cognitive security. The authors synthesize research on why people fall victim to false or deceptive information, proposing that certain brain systems are more exploitable than others. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Understanding Neurocognitive Mechanisms**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Understanding Neurocognitive Mechanisms of Cognitive**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Understanding Neurocognitive Mechanisms** work as an **epistemic-integrity review packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Understanding Neurocognitive Mechanisms**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **Understanding Neurocognitive Mechanisms** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

53.2.2.2 Lesson 2: Executive Brain Systems and Vulnerability to Information Threats Concept. Executive Brain Systems and Vulnerability to Information Threats treats the vulnerability record as an assurance case: severity, affected component, provenance, mitigation status, and uncertainty stay separate.

Why it matters. Executive Brain Systems matters in the **Cognitive Security and Influence Resilience** lane because information-integrity analysis and resilience education evidence must stay separate from judgment; treating resilience labels as permission to skip provenance review is a common failure.

Source support. Executive Brain Systems and Vulnerability to Information Threats rests on [177, 2026]. The closest source to this row notes: The authors synthesize research on why people fall victim to false or deceptive information, proposing that certain brain systems are more exploitable than others. Use it for the claim that **Executive Brain Systems and Vulnerability to Information Threats** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Read **Executive Brain Systems** against the works cited for this row. [177, 2026] A peer-reviewed review article published in Neuroscience & Biobehavioral Reviews (December 2025) by Crum and colleagues examining the neurocognitive mechanisms of cognitive security. The authors synthesize research on why people fall victim to false or deceptive information, proposing that certain brain systems are more exploitable than others. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Executive Brain Systems**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Executive Brain Systems and Vulnerability**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Executive Brain Systems** work as an **epistemic-integrity review packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Executive Brain Systems**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Apply this module's safe boundary for **Executive Brain Systems** to another artifact while keeping information-integrity analysis and resilience education and reviewer ownership explicit.

53.2.2.3 Lesson 3: Affective Systems: Emotional Exploitation in Manipulation Concept. Affective Systems: Emotional Exploitation in Manipulation focuses on transparent resilience education: provenance, audience harm, attribution caution, and non-manipulative response options.

Why it matters. Affective Systems connects classroom vocabulary to Cognitive Security and Influence Resilience practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Affective Systems: Emotional Exploitation in Manipulation rests on [177, 2026]. The most specific cited work observes: The authors synthesize research on why people fall victim to false or deceptive information, proposing that certain brain systems are more exploitable

than others. Use it for pinning down the scope of **Affective Systems: Emotional Exploitation in Manipulation**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Affective Systems**, reason from the sources cited in this row. [177, 2026] A peer-reviewed review article published in Neuroscience & Biobehavioral Reviews (December 2025) by Crum and colleagues examining the neurocognitive mechanisms of cognitive security. The authors synthesize research on why people fall victim to false or deceptive information, proposing that certain brain systems are more exploitable than others. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Affective Systems**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Affective Systems**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Affective Systems** work as an **epistemic-integrity review packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Affective Systems**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **Affective Systems** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

53.2.2.4 Lesson 4: Integrative Systems: Brain Network Interactions During Threat Exposure Concept. Integrative Systems: Brain Network Interactions During Threat Exposure connects cognitive science claims to analytic bias literacy: what the brain prioritizes, what it misses, and how review compensates.

Why it matters. Without explicit treatment of **Integrative Systems**, treating resilience labels as permission to skip provenance review undermines information-integrity analysis and resilience education review; the lesson builds the habit to separate analysis of influence from persuasion design.

Source support. Integrative Systems: Brain Network Interactions During Threat Exposure rests on [177, 2026]. The most specific cited work observes: A peer-reviewed review article published in Neuroscience & Biobehavioral Reviews (December 2025) by Crum and colleagues examining the neurocognitive mechanisms of cognitive security. Use it for pinning down the scope of **Integrative Systems: Brain Network Interactions During Threat Exposure**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Integrative Systems**, reason from the sources cited in this row. [177, 2026] A peer-reviewed review article published in Neuroscience & Biobehavioral Reviews (December 2025) by Crum and colleagues examining the neurocognitive mechanisms of cognitive security. The authors synthesize research on why people fall victim to false or deceptive information, proposing that certain brain systems are more exploitable than others. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Integrative Systems**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Integrative Systems**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Integrative Systems** work as an **epistemic-integrity review packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Integrative Systems**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Apply this module's safe boundary for **Integrative Systems** to another artifact while keeping information-integrity analysis and resilience education and reviewer ownership explicit.

53.2.2.5 Lesson 5: Neuromarkers of Susceptibility and Resilience Concept. Neuromarkers of Susceptibility and Resilience focuses on transparent resilience education: provenance, audience harm, attribution caution, and non-manipulative response options.

Why it matters. Neuromarkers of Susceptibility and Resilience connects classroom vocabulary to Cognitive Security and Influence Resilience practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Neuromarkers of Susceptibility and Resilience rests on [177, 2026]. The lead source's own note reads: A peer-reviewed review article published in Neuroscience & Biobehavioral Reviews (December 2025) by Crum and colleagues examining the neurocognitive mechanisms of cognitive security. Use it for pinning down the scope of **Neuromarkers of Susceptibility and Resilience**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Read **Neuromarkers of Susceptibility and Resilience** against the works cited for this row. [177, 2026] A peer-reviewed review article published in Neuroscience & Biobehavioral Reviews (December 2025) by Crum and colleagues examining the neurocognitive mechanisms of cognitive security. The authors synthesize research on why people fall victim to false or deceptive information, proposing that certain brain systems are more exploitable than others. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. Build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Neuromarkers of Susceptibility and Resilience**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape this subject work as an **epistemic-integrity review packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Neuromarkers of Susceptibility and Resilience**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Apply this module's safe boundary for **Neuromarkers of Susceptibility and Resilience** to another artifact while keeping information-integrity analysis and resilience education and reviewer ownership explicit.

53.2.2.6 Lesson 6: Neuro-Cognitive Approaches to Cybersecurity: Systematic Review (Emerald, 2025) Concept. Neuro-Cognitive Approaches to Cybersecurity: Systematic Review (Emerald, 2025) connects neurocognitive claims to analytic bias literacy and review compensation—not operational timing advice.

Why it matters. Without explicit treatment of **Neuro-Cognitive Approaches to Cybersecurity**, treating resilience labels as permission to skip provenance review undermines information-integrity analysis and resilience education review; the lesson builds the habit to separate analysis of influence from persuasion design.

Source support. Neuro-Cognitive Approaches to Cybersecurity: Systematic Review (Emerald, 2025) rests on [178, 2026]. Its anchor reference records: A January 2026 systematic review in Information and Computer Security by the researcher Kritika, titled "Neuro-cognitive approaches to cybersecurity." It integrates findings from neuroscience and cognitive psychology to analyze the human factor in security, examining how cognitive and neurological insights can improve security awareness education, behavioral policy development, insider threat detection, and user interface design. Use it for the working definition that **Neuro-Cognitive Approaches to Cybersecurity: Systematic Review (Emerald, 2025)** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Neuro-Cognitive Approaches to Cybersecurity**, work from the cited evidence behind this row. [178, 2026] A January 2026 systematic review in Information and Computer Security by the researcher Kritika, titled "Neuro-cognitive approaches to cybersecurity." It integrates findings from neuroscience and cognitive psychology to analyze the human factor in security, examining how cognitive and neurological insights can improve security awareness education, behavioral policy development, insider threat detection, and user interface design. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Neuro-Cognitive Approaches to Cybersecurity**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Neuro-Cognitive Approaches to Cybersecurity**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Neuro-Cognitive Approaches to Cybersecurity** work as an **epistemic-integrity review packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Neuro-Cognitive Approaches to Cybersecurity**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **Neuro-Cognitive Approaches to Cybersecurity** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

53.2.2.7 Lesson 7: Cognitive Load in Intelligence Community Settings (NCSU Survey, 2024)

Concept. Cognitive Load in Intelligence Community Settings (NCSU Survey, 2024) maps the theory to institutions: priorities, feedback, incentives, review loops, and records shape what an intelligence community notices and ignores.

Why it matters. Without explicit treatment of **Cognitive Load**, counter-messaging as manipulation undermines information-integrity analysis and resilience education review; the lesson builds the habit to separate analysis of influence from persuasion design.

Source support. Cognitive Load in Intelligence Community Settings (NCSU Survey, 2024) rests on [179, 2026]. The most specific cited work observes: Reviewing 125 articles published between 1998 and 2024, it identifies 129 distinct metrics grouped into non-biometric methods (questionnaires such as NASA-TLX, task performance, interaction tracking) and biometric methods (eye tracking, heart rate). Use it for the working definition that **Cognitive Load in Intelligence Community Settings (NCSU Survey, 2024)** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Cognitive Load**, reason from the sources cited in this row. [179, 2026] An NCSU Laboratory for Analytic Sciences article summarizing a systematic survey of metrics for measuring cognitive load in intelligence-analysis and similar settings. Reviewing 125 articles published between 1998 and 2024, it identifies 129 distinct metrics grouped into non-biometric methods (questionnaires such as NASA-TLX, task performance, interaction tracking) and biometric methods (eye tracking, heart rate). Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Cognitive Load**, build an institutional feedback-loop map with incentives, review points, and oversight hooks. Shape **Cognitive Load** work as an **epistemic-integrity review packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Cognitive Load**: that feeling certain in the moment substitutes for the checklist, pause, and second-look that decision hygiene exists to enforce.

Transfer task. Transfer **Cognitive Load** from this module to a second motif by preserving information-integrity analysis and resilience education, replacing action with audit, and naming the blocked use.

53.2.2.8 Lesson 8: 129 Metrics Catalogued: Questionnaire, Biometric, Task-Performance

Concept. 129 Metrics Catalogued: Questionnaire, Biometric, Task-Performance evaluates biometric monitoring by consent, minimization, purpose limits, and human review of alerts.

Why it matters. Without explicit treatment of **129 Metrics Catalogued**, treating resilience labels as permission to skip provenance review undermines information-integrity analysis and resilience education review; the lesson builds the habit to separate analysis of influence from persuasion design.

Source support. 129 Metrics Catalogued: Questionnaire, Biometric, Task-Performance rests on [179, 2026]. The lead source's own note reads: An NCSU Laboratory for Analytic Sciences article summarizing a systematic survey of metrics for measuring cognitive load in intelligence-analysis and similar settings. Use it for fixing what **129 Metrics Catalogued: Questionnaire, Biometric, Task-Performance** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **129 Metrics Catalogued**, work from the cited evidence behind this row. [179, 2026] An NCSU Laboratory for Analytic Sciences article summarizing a systematic survey of metrics for measuring cognitive load in intelligence-analysis and similar settings. Reviewing 125 articles published between 1998 and 2024, it identifies 129 distinct metrics grouped into non-biometric methods (questionnaires such as NASA-TLX, task performance, interaction tracking) and biometric methods (eye tracking, heart rate). Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **129 Metrics Catalogued**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **129 Metrics Catalogued**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **129 Metrics Catalogued** work as an **epistemic-integrity review packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **129 Metrics Catalogued**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Transfer **129 Metrics Catalogued** from this module to a second motif by preserving information-integrity analysis and resilience education, replacing action with audit, and naming the blocked use.

53.2.2.9 Lesson 9: NASA-TLX and Its Intelligence Analytic Applications

Concept. NASA-TLX and Its Intelligence Analytic Applications uses workload indexes as review triggers for prioritization, handoff, and rest—not as heroics metrics.

Why it matters. NASA-TLX and Its Intelligence Analytic Applications connects classroom vocabulary to Cognitive Security and Influence Resilience practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. NASA-TLX and Its Intelligence Analytic Applications rests on [179, 2026]. Its anchor reference records: An NCSU Laboratory for Analytic Sciences article summarizing a systematic survey of metrics for measuring cognitive load in intelligence-analysis and similar settings. Use it for pinning down the scope of **NASA-TLX and Its Intelligence Analytic Applications**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **NASA-TLX and Its Intelligence Analytic Applications**, reason from the sources cited in this row. [179, 2026] An NCSU Laboratory for Analytic Sciences article summarizing a systematic survey of metrics for measuring cognitive load in intelligence-analysis and similar settings. Reviewing 125 articles published between 1998 and 2024, it identifies 129 distinct metrics grouped into non-biometric methods (questionnaires such as NASA-TLX, task performance, interaction tracking) and biometric methods (eye tracking, heart rate). From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **NASA-TLX and Its Intelligence Analytic Applications**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **NASA-TLX and Its Intelligence Analytic**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape this subject work as an **epistemic-integrity review packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **NASA-TLX and Its Intelligence Analytic Applications**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Transfer **NASA-TLX and Its Intelligence Analytic Applications** from this module to a second motif by preserving information-integrity analysis and resilience education, replacing action with audit, and naming the blocked use.

53.2.2.10 Lesson 10: Eye Tracking and Heart Rate Variability for Analyst Overload Detection **Concept. Eye Tracking and Heart Rate Variability for Analyst Overload Detection** focuses on transparent resilience education: provenance, audience harm, attribution caution, and non-manipulative response options.

Why it matters. Analysts use **Eye Tracking and Heart Rate Variability for Analyst Overload Detection** to separate analysis of influence from persuasion design. A defensible treatment names the judgment it enables for information-integrity analysis and resilience education review, the proof limit that treating resilience labels as permission to skip provenance review would otherwise hide, and the reviewer accountable for challenge.

Source support. Eye Tracking and Heart Rate Variability for Analyst Overload Detection rests on [179, 2026]. The most specific cited work observes: Reviewing 125 articles published between 1998 and 2024, it identifies 129 distinct metrics grouped into non-biometric methods (questionnaires such as NASA-TLX, task performance, interaction tracking) and biometric methods (eye tracking, heart rate). Use it for pinning down the scope of **Eye Tracking and Heart Rate Variability for Analyst Overload Detection**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Ground **Eye Tracking and Heart Rate Variability for Analyst Overload Detection** in the evidence the row cites. [179, 2026] An NCSU Laboratory for Analytic Sciences article summarizing a systematic survey of metrics for measuring cognitive load in intelligence-analysis and similar settings. Reviewing 125 articles published between 1998 and 2024, it identifies 129 distinct metrics grouped into non-biometric methods (questionnaires such as NASA-TLX, task performance, interaction tracking) and biometric methods (eye tracking, heart rate). Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Eye Tracking**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Eye Tracking and Heart Rate**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Eye Tracking and Heart Rate Variability for Analyst Overload Detection** work as an **epistemic-integrity review packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Eye Tracking and Heart Rate Variability for Analyst Overload Detection**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Apply this module's safe boundary for **Eye Tracking and Heart Rate Variability for Analyst Overload Detection** to another artifact while keeping information-integrity analysis and resilience education and reviewer ownership explicit.

53.2.2.11 Lesson 11: Information Overload and Cognitive Bias in Intelligence Analysis **Concept. Information Overload and Cognitive Bias in Intelligence Analysis** manages workload and bias through prioritization, explicit handoffs, and review checkpoints—not unsustainable pace.

Why it matters. Information Overload connects classroom vocabulary to Cognitive Security and Influence Resilience practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Information Overload and Cognitive Bias in Intelligence Analysis rests on [180, 2026]. The closest source to this row notes: Heuer Jr.'s 1999 work Psychology of Intelligence Analysis and arguing for its continued relevance. Use it for pinning down the scope of **Information Overload and Cognitive Bias in Intelligence Analysis**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Information Overload**, reason from the sources cited in this row. [180, 2026] A SpecialEurasia article (2024) reviewing Richards J. Heuer Jr.'s 1999 work Psychology of Intelligence Analysis and arguing for its continued relevance. It summarizes Heuer's account of how cognitive biases such as confirmation bias, anchoring, and availability heuristics distort analytic judgment, and how analysts' backgrounds shape interpretation. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Information Overload**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must note the workload descriptor, the bounded claim about **Information Overload and Cognitive Bias**, the fatigue caveat, the uncertainty margin, the do-not-escalate boundary, and the reviewer who owns the handoff. Shape **Information Overload** work as an **epistemic-integrity review packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Information Overload**: that feeling certain in the moment substitutes for the checklist, pause, and second-look that decision hygiene exists to enforce.

Transfer task. Apply this module's safe boundary for **Information Overload** to another artifact while keeping information-integrity analysis and resilience education and reviewer ownership explicit.

53.2.2.12 Lesson 12: Decision-Making Under Uncertainty: Neural Mechanisms and Intelligence Implications **Concept. Decision-Making Under Uncertainty: Neural Mechanisms and Intelligence Implications** focuses on transparent resilience education: provenance, audience harm, attribution caution, and non-manipulative response options.

Why it matters. Decision-Making Under Uncertainty connects classroom vocabulary to Cognitive Security and Influence Resilience practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Decision-Making Under Uncertainty: Neural Mechanisms and Intelligence Implications rests on [308, 2026] and [311, 2026]. The lead source's own note reads: It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering. Use them for fixing what **Decision-Making Under Uncertainty: Neural Mechanisms and Intelligence Implications** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Decision-Making Under Uncertainty**, work from the cited evidence behind this row. [308, 2026] An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure. [311, 2026] An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Decision-Making Under Uncertainty**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Decision-Making Under Uncertainty**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Decision-Making Under Uncertainty** work as an **epistemic-integrity review packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Decision-Making Under Uncertainty**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Apply this module's safe boundary for **Decision-Making Under Uncertainty** to another artifact while keeping information-integrity analysis and resilience education and reviewer ownership explicit.

53.2.3 Neurocognitive Mechanisms of Cognitive Security worked safe example: synthetic inputs, evidence, and review

Worked example: a sample public-library class evaluates a synthetic rumor about a community service and compares transparent correction options. [238, 2026]; [240, 2026].

Triangulation anchors. In module 38's worked-example section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **cognitive resilience and epistemic integrity**. Learners use a **epistemic-integrity review packet** and keep this boundary visible: No manipulation, covert persuasion, medicalized claims, or population-level targeting.

Frame. The classroom question centers on **Understanding Neurocognitive Mechanisms of Cognitive Security (Neuroscience & Biobehavioral Reviews, 2025)**. Excluded actions stay explicit, and the **Cognitive-Resilience Lens** planning question is: How does the module protect autonomy, attention, trust, and decision quality without designing persuasion?

Inputs. For the **Understanding Neurocognitive Mechanisms of Cognitive Security** scenario, use sample posts, source timestamps, public-service facts, and a media-literacy rubric. The Cognitive-Resilience Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Understanding Neurocognitive Mechanisms of Cognitive Security**, students trace narrative provenance, separate observation from attribution, name audience harms, and design a transparent lesson. Pause whenever an inference about Understanding the module appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Understanding Neurocognitive Mechanisms of Cognitive Security** classroom scenario; unit artifact = epistemic-integrity review packet; evidence = allowed inputs; method = information-integrity analysis and resilience education; output = a narrative-risk map with caveats, response options, and no microtargeted persuasion; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Understanding Neurocognitive Mechanisms of Cognitive Security** as "Cognitive-Resilience Lens confirms it" is not enough. The revision ties the claim to information-integrity analysis and resilience education, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Understanding Neurocognitive Mechanisms of Cognitive Security** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

53.2.4 Neurocognitive Mechanisms of Cognitive Security practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Cognitive-Resilience Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats**.

Triangulation anchors. In module 38's practice-sequence section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Understanding Neurocognitive Mechanisms of Cognitive Security, Executive Brain Systems and Vulnerability to Information Threats, Affective Systems: Emotional Exploitation in Manipulation; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Cognitive Security and Influence Resilience** lane.
2. Frame	Answer the lens question: How does the module protect autonomy, attention, trust, and decision quality without designing persuasion?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Understanding Neurocognitive Mechanisms of Cognitive Security: narrative-risk map with provenance, uncertainty, audience harms, and response options.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the epistemic-integrity review packet fields for Understanding Neurocognitive Mechanisms of Cognitive Security.	Unit profile note.	Evidence artifacts include provenance chain, correction option.
4. Challenge	Test the misconception that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.	Failure-mode note.	The artifact applies the key distinction: separate analysis of influence from persuasion design.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

53.2.4.1 Neurocognitive Mechanisms of Cognitive Security instructor notes: source reasoning, review points, and studio focus

Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats**. [238, 2026]; [240, 2026].

53.2.4.2 Neurocognitive Mechanisms of Cognitive Security extension exercise: peer validation and refresh trigger review

Evidence anchor. Section 53; [238, 2026].

Have learners swap artifacts and apply the **Cognitive-Resilience Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats**.

53.2.5 Neurocognitive Mechanisms of Cognitive Security knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 53; [238, 2026].

1. Explain how **Understanding Neurocognitive Mechanisms of Cognitive Security (Neuroscience & Biobehavioral Reviews, 2025)** is defined here; name the source descriptor that supports the definition.
2. Contrast **Understanding Neurocognitive Mechanisms of Cognitive Security** with **Executive Brain Systems and Vulnerability to Information Threats** using the **Cognitive-Resilience Lens** artifact fields.
3. Identify one failure mode from the **Cognitive Security and Influence Resilience** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which response informs people without crossing into MISO-style manipulation or unverified attribution?
5. Correct this misconception: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

53.2.5.1 Neurocognitive Mechanisms of Cognitive Security answer quality rubric: source evidence, uncertainty, and safe transfer

Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Understanding Neurocognitive Mechanisms of Cognitive Security** without source evidence, uncertainty, or a safe transfer task.

53.3 Neurocognitive Mechanisms of Cognitive Security assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 53; [238, 2026].

53.3.1 Neurocognitive Mechanisms of Cognitive Security evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 53; [238, 2026].

53.3.2 Neurocognitive Mechanisms of Cognitive Security transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 53; [238, 2026].

53.3.2.1 Neurocognitive Mechanisms of Cognitive Security lineage and source tradition: profile, concepts, and first anchors This sits in the **Cognitive Security and Influence Resilience** lineage: protecting attention, belief formation, and decision quality without turning resilience education into manipulation. [238, 2026]; [240, 2026].

53.3.2.2 Neurocognitive Mechanisms of Cognitive Security working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 53; [238, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats**, with provenance and reviewability throughout.

53.3.2.3 Neurocognitive Mechanisms of Cognitive Security knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [238, 2026]; [240, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

53.3.2.4 Neurocognitive Mechanisms of Cognitive Security transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 53; [238, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats**.
- **Evidence contract:** keep the **Cognitive Security and Influence Resilience** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

53.3.2.5 Neurocognitive Mechanisms of Cognitive Security profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 53; [238, 2026].

The matched profile emphasizes protecting attention, belief formation, and decision quality without turning resilience education into manipulation. The method stack is claim decomposition, narrative provenance, inoculation framing, bias checks, audience-risk review, and after-action learning; the local topic cluster is **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats**.

53.3.3 Neurocognitive Mechanisms of Cognitive Security evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 53; [238, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Cognitive Security and Influence Resilience** profile tells reviewers what evidence is strong enough for the module artifact built around **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats**.

53.3.3.1 Neurocognitive Mechanisms of Cognitive Security guide source spine: inherited keys and local citation roles Primary guide citations: [238, 2026]; [240, 2026]; [244, 2026]; [274, 2026]; [278, 2026]; [280, 2026]; [287, 2026]; [288, 2026]; [295, 2026]; [176, 2026]; [177, 2026]; [178, 2026]; [179, 2026]; [180, 2026]; [308, 2026]; [311, 2026].

53.3.3.2 Neurocognitive Mechanisms of Cognitive Security verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [238, 2026]; [240, 2026].

Tier	What counts	How it is used
Source guide	[238, 2026]; [240, 2026]; [244, 2026]; [274, 2026]; [278, 2026]; [280, 2026]; [287, 2026]; [288, 2026]; [295, 2026]; [176, 2026]; [177, 2026]; [178, 2026]; [179, 2026]; [180, 2026]; [308, 2026]; [311, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 38's source-canon section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats** and [238, 2026]; [240, 2026], but only directly verified source URLs are encoded as citations.

53.3.3.3 Neurocognitive Mechanisms of Cognitive Security intelligence practice lens: evidence artifact and safety check Practice lens: **Cognitive-Resilience Lens** for **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats**. [238, 2026]; [240, 2026].

Planning question: How does the module protect autonomy, attention, trust, and decision quality without designing persuasion?

Evidence artifact: narrative-risk map with provenance, uncertainty, audience harms, and response options.

Validation rule: distinguish observation, attribution, impact assessment, and resilience response. Applied to **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats**.

Handoff contract: handoff supports transparency, education, and resilience, not microtargeted influence or deception.

Safety check: exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning.

53.3.3.4 Neurocognitive Mechanisms of Cognitive Security runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 53; [238, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	38.99	38.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Neurocognitive Mechanisms of Cognitive Security to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Bounded autonomy, procurement, incident-response, and assurance studio	38.101	38.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Neurocognitive Mechanisms of Cognitive Security	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Model-card, recoverability, retention, and learner-support evidence package	38.102	38.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Neurocognitive Mechanisms of Cognitive Security	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Understanding Neurocognitive Mechanisms of Cognitive Security (Neuroscience & Biobehavioral Reviews, 2025)	38.1	38.1 Understanding Neurocognitive Mechanisms of Cognitive Security (Neuroscience & Biobehavioral Reviews, 2025)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Executive Brain Systems and Vulnerability to Information Threats	38.1.1	38.1.1 Executive Brain Systems and Vulnerability to Information Threats	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Affective Systems: Emotional Exploitation in Manipulation	38.1.2	38.1.2 Affective Systems: Emotional Exploitation in Manipulation	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Integrative Systems: Brain Network Interactions During Threat Exposure	38.1.3	38.1.3 Integrative Systems: Brain Network Interactions During Threat Exposure	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Neuromarkers of Susceptibility and Resilience	38.1.4	38.1.4 Neuromarkers of Susceptibility and Resilience	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Neuro-Cognitive Approaches to Cybersecurity: Systematic Review (Emerald, 2025)	38.2	38.2 Neuro-Cognitive Approaches to Cybersecurity: Systematic Review (Emerald, 2025)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Cognitive Load in Intelligence Community Settings (NCSU Survey, 2024)	38.3	38.3 Cognitive Load in Intelligence Community Settings (NCSU Survey, 2024)	Operator-Workload Hygiene Lens	operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary	exclude live operational tempo mandates, surveillance of people, performance coercion, and unreviewed tasking under fatigue
129 Metrics Catalogued: Questionnaire, Biometric, Task-Performance	38.3.1	38.3.1 129 Metrics Catalogued: Questionnaire, Biometric, Task-Performance	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
NASA-TLX and Its Intelligence Analytic Applications	38.3.2	38.3.2 NASA-TLX and Its Intelligence Analytic Applications	Operator-Workload Hygiene Lens	operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary	exclude live operational tempo mandates, surveillance of people, performance coercion, and unreviewed tasking under fatigue
Eye Tracking and Heart Rate Variability for Analyst Overload Detection	38.3.3	38.3.3 Eye Tracking and Heart Rate Variability for Analyst Overload Detection	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Information Overload and Cognitive Bias in Intelligence Analysis	38.4	38.4 Information Overload and Cognitive Bias in Intelligence Analysis	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Decision-Making Under Uncertainty: Neural Mechanisms and Intelligence Implications	38.5	38.5 Decision-Making Under Uncertainty: Neural Mechanisms and Intelligence Implications	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning

53.3.3.5 Neurocognitive Mechanisms of Cognitive Security reusable subsection contract: topic rows, artifacts, and safety duties Evidence anchor. Section 53; [238, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Understanding Neurocognitive Mechanisms of Cognitive Security (Neuroscience & Biobehavioral Reviews, 2025)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Executive Brain Systems and Vulnerability to Information Threats	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning

Lesson topic	Practice lens	Evidence artifact	Safety check
Affective Systems: Emotional Exploitation in Manipulation	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Integrative Systems: Brain Network Interactions During Threat Exposure	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Neuromarkers of Susceptibility and Resilience	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Neuro-Cognitive Approaches to Cybersecurity: Systematic Review (Emerald, 2025)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Cognitive Load in Intelligence Community Settings (NCSU Survey, 2024)	Operator-Workload Hygiene Lens	operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary	exclude live operational tempo mandates, surveillance of people, performance coercion, and unreviewed tasking under fatigue
129 Metrics Catalogued: Questionnaire, Biometric, Task-Performance	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
NASA-TLX and Its Intelligence Analytic Applications	Operator-Workload Hygiene Lens	operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary	exclude live operational tempo mandates, surveillance of people, performance coercion, and unreviewed tasking under fatigue
Eye Tracking and Heart Rate Variability for Analyst Overload Detection	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Information Overload and Cognitive Bias in Intelligence Analysis	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Decision-Making Under Uncertainty: Neural Mechanisms and Intelligence Implications	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning

53.3.3.6 Neurocognitive Mechanisms of Cognitive Security annotated source ledger: real titles and local contribution Each source cited by this **Cognitive Security and Influence Resilience** module is paired below with its real title and a one-line note on what it contributes to **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats**.

Source	Cited work	What it contributes	Status
[238, 2026]	Recommendation on the Ethics of Artificial Intelligence	The official UNESCO page for the Recommendation on the Ethics of Artificial Intelligence, the first global standard-setting instrument on AI ethics, adopted in 2021 and applicable to all 194 member states. It outlines four core values, including human rights protection and environmental flourishing, and ten guiding principles such as proportionality, privacy, transparency, and fairness.	verified source-guide
[240, 2026]	The Right to Privacy in the Digital Age	The Office of the High Commissioner for Human Rights (OHCHR) hub page on the right to privacy in the digital age. It addresses how data-intensive technologies, particularly artificial intelligence, create risks for privacy, autonomy, and human dignity, and curates international standards, reports, and expert consultations.	verified source-guide
[244, 2026]	AI and Education	Official UNESCO GEM AI and education source hub.	original source-guide

Source	Cited work	What it contributes	Status
[274, 2026]	CAST Universal Design for Learning Guidelines version 3.0	The official CAST website for the Universal Design for Learning (UDL) Guidelines version 3.0, released in 2024. The framework offers research-based guidance for designing inclusive learning environments and is organized around three principles: Engagement (motivation and emotional support), Representation (accessible presentation of information), and Action and Expression (diverse means of participation and communication).	verified source-guide
[278, 2026]	Recommendation of the Council on Public Procurement	The OECD Recommendation of the Council on Public Procurement (OECD/LEGAL/0411), a legal instrument adopted by the OECD Council in 2015 on the proposal of the Public Governance Committee. It frames public procurement as a pillar of strategic governance and service delivery and sets out principles for governments to follow.	verified source-guide
[280, 2026]	NIST SP 800-61 Rev. 3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management	NIST SP 800-61 Rev. 3, published April 2025, integrates incident response guidance into broader cybersecurity risk management aligned with the NIST Cybersecurity Framework 2.0, superseding the 2012 Rev. 2. The publication addresses cyber threat information sharing, incident handling and management practices, and procedures for detecting, responding to, and recovering from security incidents.	verified source-guide
[287, 2026]	Datasheets for Datasets	A 2018 arXiv paper proposing 'datasheets for datasets,' a standardized documentation framework for machine learning datasets modeled on electronic component datasheets. The authors argue the field lacks consistent dataset documentation, which creates risk in high-stakes applications, and propose that datasets be accompanied by documentation covering motivation, composition, collection process, recommended uses, and test results.	verified source-guide
[288, 2026]	Algorithmic Transparency Recording Standard Hub	A GOV.UK collection page serving as the hub for the UK Algorithmic Transparency Recording Standard (ATRS), maintained by the Government Digital Service. It provides a standardized template for documenting public-sector use of algorithmic tools, completion guidance, policy on scope and compliance, and a searchable repository of published transparency records.	verified source-guide
[295, 2026]	M-25-22: Driving Efficient Acquisition of Artificial Intelligence in Government	OMB Memorandum M-25-22 (April 3, 2025), Driving Efficient Acquisition of Artificial Intelligence in Government, issued under Executive Order 13960 and related directives. It provides guidance to federal agencies for acquiring effective and trustworthy AI in a timely, cost-effective manner, and rescinds and replaces earlier memorandum M-24-18.	verified source-guide

Source	Cited work	What it contributes	Status
[176, 2026]	Understanding the Neurocognitive Mechanisms of Cognitive Security	Cognitive security is a relatively new field that aims to understand and defend against.	original source-guide
[177, 2026]	Understanding the neurocognitive mechanisms of cognitive security	A peer-reviewed review article published in Neuroscience & Biobehavioral Reviews (December 2025) by Crum and colleagues examining the neurocognitive mechanisms of cognitive security. The authors synthesize research on why people fall victim to false or deceptive information, proposing that certain brain systems are more exploitable than others.	verified source-guide
[178, 2026]	Neuro-cognitive approaches to cybersecurity: a systematic review	A January 2026 systematic review in Information and Computer Security by the researcher Kritika, titled "Neuro-cognitive approaches to cybersecurity." It integrates findings from neuroscience and cognitive psychology to analyze the human factor in security, examining how cognitive and neurological insights can improve security awareness education, behavioral policy development, insider threat detection, and user interface design.	verified source-guide
[179, 2026]	Survey of Metrics for Cognitive Load in Intelligence Community	An NCSU Laboratory for Analytic Sciences article summarizing a systematic survey of metrics for measuring cognitive load in intelligence-analysis and similar settings. Reviewing 125 articles published between 1998 and 2024, it identifies 129 distinct metrics grouped into non-biometric methods (questionnaires such as NASA-TLX, task performance, interaction tracking) and biometric methods (eye tracking, heart rate).	verified source-guide
[180, 2026]	Why Psychology of Intelligence Analysis Still Matters?	A SpecialEurasia article (2024) reviewing Richards J. Heuer Jr.'s 1999 work Psychology of Intelligence Analysis and arguing for its continued relevance. It summarizes Heuer's account of how cognitive biases such as confirmation bias, anchoring, and availability heuristics distort analytic judgment, and how analysts' backgrounds shape interpretation.	verified source-guide context; do not use as primary analytic support
[308, 2026]	Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure	An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure.	verified source-guide
[311, 2026]	Countering Information Threats	An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering.	verified source-guide

Where this sits. This module's overview is Section 53; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

53.3.4 Neurocognitive Mechanisms of Cognitive Security governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 53; [238, 2026].

53.3.5 Neurocognitive Mechanisms of Cognitive Security analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 38's governance-boundary section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **Cognitive Security and Influence Resilience** for **Understanding Neurocognitive Mechanisms of Cognitive Security (Neuroscience & Biobehavioral Reviews, 2025); Executive Brain Systems and Vulnerability to Information Threats**. [238, 2026]; [240, 2026].

Curriculum topic spine: Understanding Neurocognitive Mechanisms of Cognitive Security (Neuroscience & Biobehavioral Reviews, 2025), **Executive Brain Systems and Vulnerability to Information Threats**, **Affective Systems: Emotional Exploitation in Manipulation**. **Verified anchor cluster:** [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]; [OECD, 2026c]; [for Security Policy, 2025]; [Community, 2020a].

Conceptual depth: protecting attention, belief formation, and decision quality without turning resilience education into manipulation.

Method stack: claim decomposition, narrative provenance, inoculation framing, bias checks, audience-risk review, and after-action learning.

Composability contract: separate descriptive analysis, normative assessment, response options, and protected-audience considerations.

Known failure modes: counter-messaging as manipulation, overclaiming intent, pathologizing audiences, and collapsing uncertainty into moral certainty.

Defensive boundary: practice uses benign simulations and resilience education; it does not create persuasion campaigns, impersonation, or deception plans. Applied to **Understanding Neurocognitive Mechanisms of Cognitive Security (Neuroscience & Biobehavioral Reviews, 2025); Executive Brain Systems and Vulnerability to Information Threats**.

Anchor	Why it matters here
[Cybersecurity and Agency, 2024b]	Official CISA guidance on foreign influence operations targeting critical infrastructure. Checked as of 2026-05-21; role: source_quality_anchor.
[Organization, 2026b]	Official NATO counter-information-threat guidance. Checked as of 2026-05-21; role: source_quality_anchor.
[Cybersecurity and Agency, 2026b]	Official CISA election-security source for public-resilience, foreign-influence awareness, rumor control, and defensive communication framing. Checked as of 2026-05-21; role: curriculum_anchor.
[Organization, 2026c]	Official NATO source for hybrid-threat resilience across cyber, information, economic, political, and military pressure. Checked as of 2026-05-21; role: curriculum_anchor.
[OECD, 2026c]	Official OECD policy source for information integrity, governance responses, public trust, and democratic resilience. Checked as of 2026-05-21; role: curriculum_anchor.
[for Security Policy, 2025]	Policy-scholarship source for cognitive security, information literacy, critical thinking, and whole-of-society resilience. Checked as of 2026-05-21; role: curriculum_anchor.
[Community, 2020a]	Official IC framework for AI goals, authorities, human judgment, bias mitigation, testing, documentation, explainability, and review. Checked as of 2026-05-21; role: curriculum_anchor.

53.3.5.1 Neurocognitive Mechanisms of Cognitive Security evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **Cognitive Security and Influence Resilience** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [238, 2026]; [240, 2026].

53.3.6 Neurocognitive Mechanisms of Cognitive Security agentic boundary: assist, approve, block, and record

Evidence anchor. Section 53; [238, 2026].

AGEINT translation is bounded by the **Cognitive Security and Influence Resilience** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats**.

53.3.6.1 Neurocognitive Mechanisms of Cognitive Security permitted defensive utility: curriculum uses and safe outputs

Evidence anchor. Section 53; [238, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats**.

53.3.6.2 Neurocognitive Mechanisms of Cognitive Security excluded operational boundary: blocked actions and stop rules

Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [238, 2026]; [240, 2026] and **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

53.3.7 Neurocognitive Mechanisms of Cognitive Security governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 53; [238, 2026].

Governance is practiced as a gate on the **Cognitive Security and Influence Resilience** lane. Learners use the **Cognitive-Resilience Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats**.

53.3.7.1 Neurocognitive Mechanisms of Cognitive Security governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [238, 2026]; [240, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Cognitive Security and Influence Resilience** failure modes and the **Cognitive-Resilience Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

53.3.7.2 Neurocognitive Mechanisms of Cognitive Security evidence package handoff: appendices, records, and reuse Evidence anchor. Section 53; [238, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Cognitive-Resilience Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats**.

53.3.7.3 Neurocognitive Mechanisms of Cognitive Security current-source assurance: verified anchors and local artifact fit The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats**. [238, 2026]; [240, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_cisa_foreign_influence` for **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats**?	Preparing for and Mitigating Foreign Influence Operations; lane `source_quality_spine`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official CISA guidance on foreign influence operations targeting critical infrastructure.
What does the module inherit from `official_nato_counter_information_threats` for **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats**?	Countering Information Threats; lane `source_quality_spine`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official NATO counter-information-threat guidance.
What does the module inherit from `official_cisa_election_security_influence` for **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats**?	Election Security; lane `cognitive_influence_security`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official CISA election-security source for public-resilience, foreign-influence awareness, rumor control, and defensive communication framing.
What does the module inherit from `official_nato_hybrid_threats` for **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats**?	Countering Hybrid Threats; lane `cognitive_influence_security`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official NATO source for hybrid-threat resilience across cyber, information, economic, political, and military pressure.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 53; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

53.3.8 Neurocognitive Mechanisms of Cognitive Security assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 53; [238, 2026].

53.3.9 Neurocognitive Mechanisms of Cognitive Security assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 53; [238, 2026].

53.3.9.1 Neurocognitive Mechanisms of Cognitive Security capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats**.
Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats** and [238, 2026]; [240, 2026].

53.3.9.2 Neurocognitive Mechanisms of Cognitive Security instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats** and [238, 2026]; [240, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

53.3.9.3 Neurocognitive Mechanisms of Cognitive Security assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Understanding Neurocognitive Mechanisms of Cognitive Security (Neuroscience & Biobehavioral Reviews, 2025)	Completed **narrative-risk map with provenance, uncertainty, audience harms, and response options** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Executive Brain Systems and Vulnerability to Information Threats	Completed **narrative-risk map with provenance, uncertainty, audience harms, and response options** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Affective Systems: Emotional Exploitation in Manipulation	Completed **narrative-risk map with provenance, uncertainty, audience harms, and response options** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

53.3.10 Neurocognitive Mechanisms of Cognitive Security refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [238, 2026]; [240, 2026] and **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats**.

53.3.10.1 Neurocognitive Mechanisms of Cognitive Security refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats**. The local signals begin with [238, 2026]; [240, 2026].

53.3.10.2 Neurocognitive Mechanisms of Cognitive Security claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats**, and the source spine for these checks begins with [238, 2026]; [240, 2026].

53.3.11 Neurocognitive Mechanisms of Cognitive Security reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [238, 2026]; [240, 2026].
Triangulation anchors. In module 38's review-checklist section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats**. [238, 2026]; [240, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

53.3.12 Neurocognitive Mechanisms of Cognitive Security learning-path links: module map, overview, and curriculum atlas

Use the cross-links below to place **Understanding Neurocognitive Mechanisms of Cognitive Security; Executive Brain Systems and Vulnerability to Information Threats** in the wider unit: the orientation sets the frame, the parent unit supplies the shared safety posture, and the neighbouring modules show what evidence enters and leaves. Lead sources: [238, 2026]; [240, 2026].

Section 2, Section 51, Section 52, Section 54

54 Psychological Inoculation and Prebunking

54.0.1 Psychological Inoculation and Prebunking figures and course links: visual evidence, source flow, and navigation

The module uses Figure 113, Figure 114, and Figure 107 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 51, Section 53, Section 55.
This module teaches the **Cognitive Security and Influence Resilience** lane through a bounded, source-backed coursebook chapter. [242, 2026]; [243, 2026].

54.1 Cognitive Security and Influence Resilience frame for Psychological Inoculation and Prebunking: source context, topic focus, and reader task

Evidence anchor. Section 54; [242, 2026].

54.1.1 Psychological Inoculation and Prebunking orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 54; [242, 2026].

54.1.2 Psychological Inoculation and Prebunking conceptual primer: source context, core model, and reader task

This chapter teaches cognitive security as protection of attention, trust, memory, and decision quality without creating manipulation. The chapter uses **Cognitive-Resilience Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**.
The central distinction is to separate analysis of influence from persuasion design. Core topics include **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy; Prebunking Interventions Based on Inoculation: Psychological inoculation and prebunking literacy**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [242, 2026]; [243, 2026].
Learners move from vocabulary and the **Cognitive-Resilience Lens** distinction through topic lessons on **Psychological inoculation and prebunking literacy** with evidence and misconception checks, then assemble a **narrative-risk map with provenance, uncertainty, audience harms, and response options** with safety and rights gates.

54.1.3 Psychological Inoculation and Prebunking learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 54; [242, 2026].

- Connect **Psychological inoculation and prebunking literacy and Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy** to **Cognitive Security and Influence Resilience** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate analysis of influence from persuasion design; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as counter-messaging as manipulation, overclaiming intent, pathologizing audiences, and collapsing uncertainty into moral certainty, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: practice uses benign simulations and resilience education; it does not create persuasion campaigns, impersonation, or deception plans.

54.1.4 Psychological Inoculation and Prebunking core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 54; [242, 2026].

Term	Working definition
Narrative provenance	where a claim, frame, or story came from and how it spread
Prebunking	transparent education that helps people recognize misleading patterns before exposure
Audience harm	a privacy, dignity, autonomy, or trust risk for people receiving information
Attribution caution	the rule that intent and origin claims need strong evidence
Resilience response	a transparent education, correction, or process improvement that avoids manipulation
MISO boundary	the line between accountable public messaging analysis and covert influence design
Inoculation	building recognition of manipulation tactics without deploying persuasion against a population
Psychological inoculation and prebunking…	Key terms: Psychological, inoculation, prebunking.
Psychological Inoculation Against…	Key terms: Psychological, Inoculation, Against.

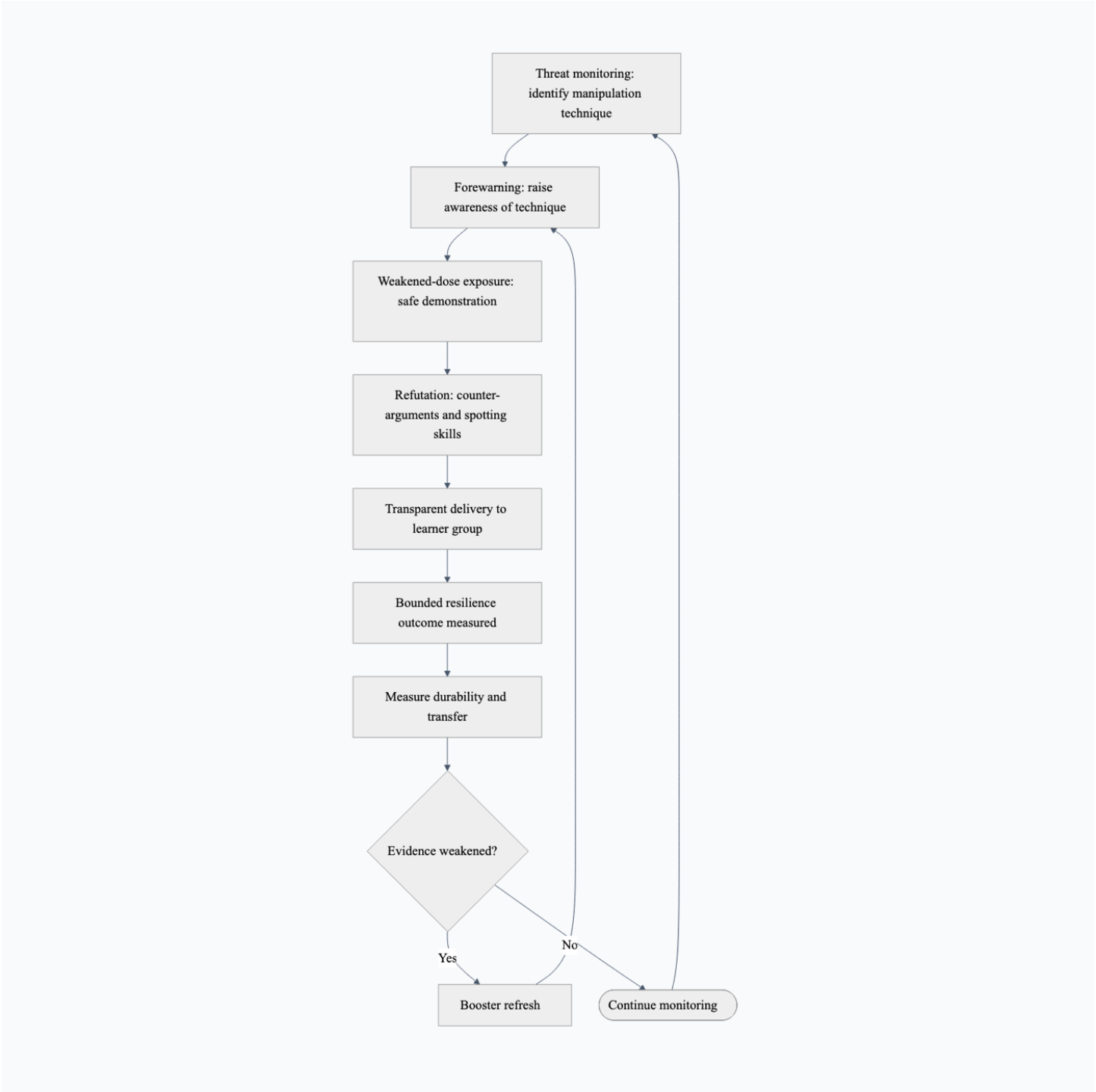


Figure 113: Conceptual defensive education schematic for transparent prebunking: effects are bounded, context-dependent, measured, and refreshed rather than assumed. Its reader value is to make A top-to-bottom educational pipeline. Monitoring identifies a manipulation technique. This feeds forewarning, a safe weakened-dose demonstration, refutation with technique-spotting skills, and transparent delivery to a learner group visible at a glance, with the cognitive security / psychological inoculation and prebunking section as the source section and defensive review as the boundary.

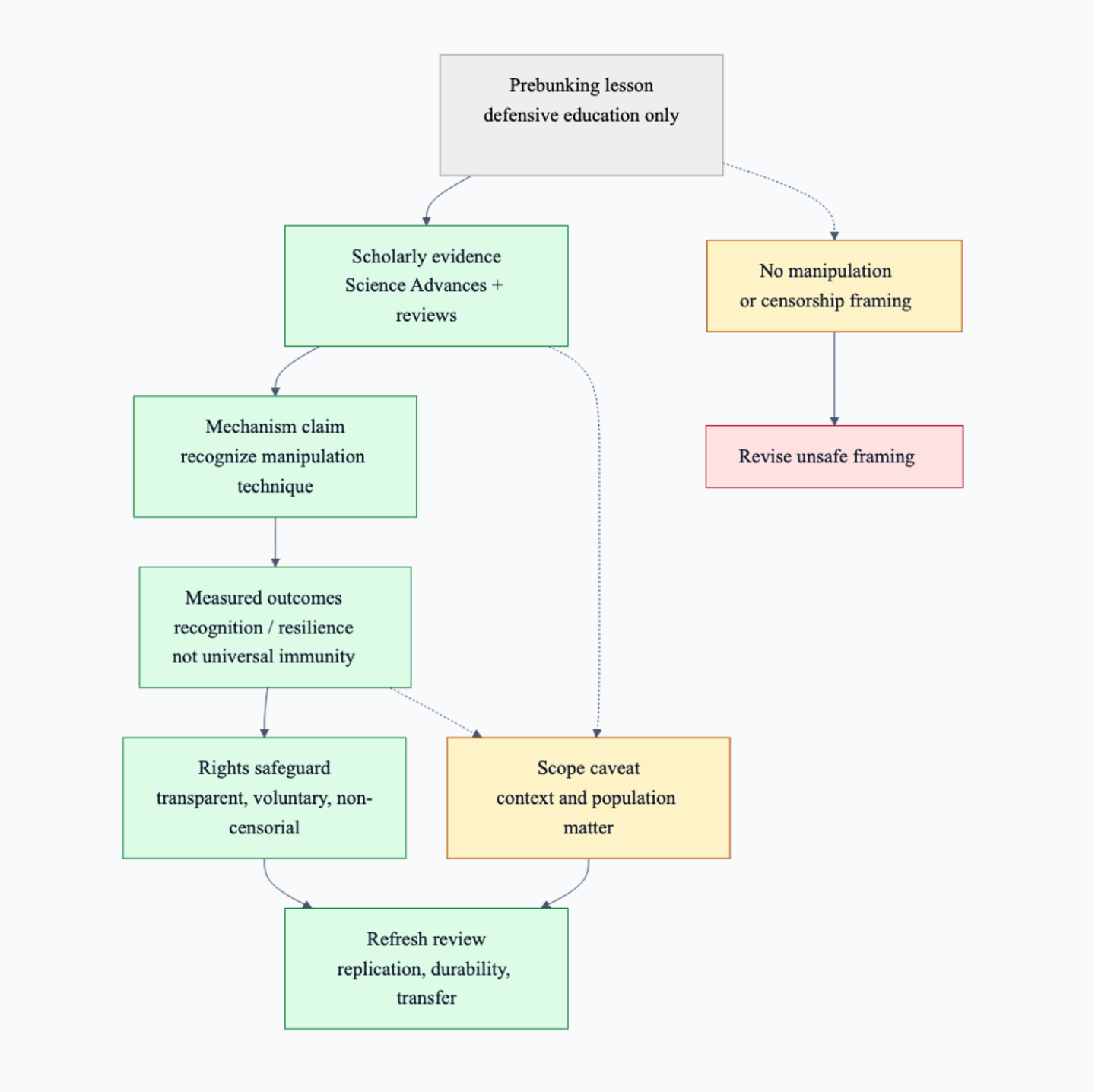


Figure 114: Source-backed conceptual schematic for bounded inoculation and prebunking claims: scholarly mechanism evidence, measured outcomes, rights safeguards, and refresh duties remain separate. The captioned view belongs to the cognitive security / psychological inoculation and prebunking section and should be read as a map of Prebunking lesson defensive education only, Scholarly evidence Science Advances + reviews, Mechanism claim recognize manipulation technique, and Measured outcomes recognition / resilience not universal immunity, not as a capability score or live-task instruction.

54.2 Cognitive-Resilience Lens path for Psychological Inoculation and Prebunking: lesson cluster, safe artifact, and review

Evidence anchor. Section 54; [242, 2026].

54.2.1 Psychological Inoculation and Prebunking practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 54; [242, 2026].

54.2.2 Psychological Inoculation and Prebunking topic lessons: source-backed concepts and transfer tasks

This module builds cognitive security as protection of attention, trust, memory, and decision quality without creating manipulation. The sequence opens with **Psychological inoculation and prebunking literacy**, **Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**, **Prebunking Interventions Based on Inoculation: Psychological inoculation and prebunking literacy** and applies the **Cognitive-Resilience Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 107; module overview Section 54; curriculum atlas Section 2.

Triangulation anchors. In module 39's topic-lessons section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

54.2.2.1 Lesson 1: Psychological inoculation and prebunking literacy **Concept. Psychological inoculation and prebunking literacy** uses inoculation methods as evidence-informed, bounded, and context-dependent resilience education with transparent labels, source checks, non-manipulative corrections, and explicit measurement limits.

Why it matters. Psychological inoculation connects classroom vocabulary to Cognitive Security and Influence Resilience practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Psychological inoculation and prebunking literacy rests on [181, 2026] and [182, 2026]. Its anchor reference records: It reports bounded improvements in people's ability to distinguish misinformation from real information, while finding limited effect on intentions to share misinformation and leaving context, durability, and transfer conditions for review. Use them for the working definition that **Psychological inoculation and prebunking literacy** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Psychological inoculation**, work from the cited evidence behind this row. [181, 2026] Particularly noteworthy in this field is the resurgence of the cognitive inoculation theory. [182, 2026] A 2023 meta-analysis in the Journal of Medical Internet Research evaluating psychological inoculation, or prebunking, as a strategy against misinformation, drawing on 42 studies with over 42,000 participants. It reports bounded improvements in people's ability to distinguish misinformation from real information, while finding limited effect on intentions to share misinformation and leaving context, durability, and transfer conditions for review. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. Build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Psychological inoculation**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape this subject work as an **epistemic-integrity review packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Psychological inoculation**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **Psychological inoculation** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

54.2.2.2 Lesson 2: Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy **Concept. Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy** analyzes influence campaigns through provenance, audience harm, attribution caution, and transparent response options.

Why it matters. Psychological Inoculation Against Misinformation connects classroom vocabulary to Cognitive Security and Influence Resilience practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy rests on [182, 2026]. Its anchor reference records: A 2023 meta-analysis in the Journal of Medical Internet Research evaluating psychological inoculation, or prebunking, as a strategy against misinformation, drawing on 42 studies with over 42,000 participants. Use it for the working definition that **Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Psychological Inoculation Against Misinformation**, reason from the sources cited in this row. [182, 2026] A 2023 meta-analysis in the Journal of Medical Internet Research evaluating psychological inoculation, or prebunking, as a strategy against misinformation, drawing on 42 studies with over 42,000 participants. It reports bounded improvements in people's ability to distinguish misinformation from real information, while finding limited effect on intentions to share misinformation and leaving context, durability, and transfer conditions for review. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Psychological Inoculation Against Misinformation**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Psychological Inoculation Against Misinformation**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Psychological Inoculation Against Misinformation** work as an **epistemic-integrity review packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Psychological Inoculation Against Misinformation**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **Psychological Inoculation Against Misinformation** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

54.2.2.3 Lesson 3: Prebunking Interventions Based on Inoculation: Psychological inoculation and prebunking literacy **Concept. Prebunking Interventions Based on Inoculation: Psychological inoculation and prebunking literacy** uses inoculation methods as evidence-informed, bounded, and context-dependent resilience education with transparent labels, source checks, non-manipulative corrections, and explicit measurement limits.

Why it matters. Without explicit treatment of **Prebunking Interventions Based on Inoculation**, treating resilience labels as permission to skip provenance review undermines information-integrity analysis and resilience education review; the lesson builds the habit to separate analysis of influence from persuasion design.

Source support. Prebunking Interventions Based on Inoculation: Psychological inoculation and prebunking literacy rests on [183, 2026]. The lead source's own note reads: A 2020 peer-reviewed study in the Harvard Kennedy School Misinformation Review by Roozenbeek, van der

Linden, and Nygren testing the Bad News game as a prebunking intervention grounded in inoculation theory. Use it for pinning down the scope of **Prebunking Interventions Based on Inoculation: Psychological inoculation and prebunking literacy**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Ground **Prebunking Interventions Based on Inoculation** in the evidence the row cites. [183, 2026] A 2020 peer-reviewed study in the Harvard Kennedy School Misinformation Review by Roozenbeek, van der Linden, and Nygren testing the Bad News game as a prebunking intervention grounded in inoculation theory. Players take the role of a misinformation creator to learn common manipulation techniques such as impersonation, emotional appeals, polarization, and conspiratorial framing, building resistance to deceptive content. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Prebunking Interventions Based on Inoculation**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Prebunking Interventions Based on Inoculation**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Prebunking Interventions Based on Inoculation** work as an **epistemic-integrity review packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Prebunking Interventions Based on Inoculation**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Transfer **Prebunking Interventions Based on Inoculation** from this module to a second motif by preserving information-integrity analysis and resilience education, replacing action with audit, and naming the blocked use.

54.2.2.4 Lesson 4: Cambridge/Jigsaw YouTube Field Study: 5.4 Million Users, 7 Experiments

Concept. Cambridge/Jigsaw YouTube Field Study: 5.4 Million Users, 7 Experiments applies Cambridge, Jigsaw, YouTube within Cognitive Security and Influence Resilience: learners use separate analysis of influence from persuasion design and information-integrity analysis and resilience education evidence before any judgment moves forward.

Why it matters. Analysts use **Cambridge/Jigsaw YouTube Field Study** to separate analysis of influence from persuasion design. A defensible treatment names the judgment it enables for information-integrity analysis and resilience education review, the proof limit that counter-messaging as manipulation would otherwise hide, and the reviewer accountable for challenge.

Source support. Cambridge/Jigsaw YouTube Field Study: 5.4 Million Users, 7 Experiments rests on [152, 2026]. The closest source to this row notes: The 90-second clips expose common manipulation techniques such as scapegoating, false dichotomies, and emotionally manipulative language, an approach the researchers call prebunking. Use it for the claim that **Cambridge/Jigsaw YouTube Field Study: 5.4 Million Users, 7 Experiments** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Read **Cambridge/Jigsaw YouTube Field Study** against the works cited for this row. [152, 2026] A University of Cambridge news article describing a large study, conducted with Bristol University and Google's Jigsaw, testing whether short animated videos can help people resist online manipulation. The 90-second clips expose common manipulation techniques such as scapegoating, false dichotomies, and emotionally manipulative language, an approach the researchers call prebunking. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Cambridge/Jigsaw YouTube Field Study**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must name the source descriptor, the bounded claim about **Cambridge/Jigsaw YouTube Field Study**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Cambridge/Jigsaw YouTube Field Study** work as an **epistemic-integrity review packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that Cambridge/Jigsaw YouTube Field Study: 5.4 Million Users, 7 Experiments establishes intent without reviewing alternative explanations.

Transfer task. Transfer **Cambridge/Jigsaw YouTube Field Study** to a second module by preserving information-integrity analysis and resilience education, changing the source evidence, and naming a new reviewer.

54.2.2.5 Lesson 5: Inoculation Effect: Psychological inoculation and prebunking literacy

Concept. Inoculation Effect: Psychological inoculation and prebunking literacy uses inoculation methods as evidence-informed, bounded, and context-dependent resilience education with transparent labels, source checks, non-manipulative corrections, and explicit measurement limits.

Why it matters. Inoculation Effect connects classroom vocabulary to Cognitive Security and Influence Resilience practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Inoculation Effect: Psychological inoculation and prebunking literacy rests on [152, 2026]. Its anchor reference records: The 90-second clips expose common manipulation techniques such as scapegoating, false dichotomies, and emotionally manipulative language, an approach the researchers call prebunking. Use it for the claim that **Inoculation Effect: Psychological inoculation and prebunking literacy** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Read **Inoculation Effect** against the works cited for this row. [152, 2026] A University of Cambridge news article describing a large study, conducted with Bristol University and Google's Jigsaw, testing whether short animated videos can help people resist online manipulation. The 90-second clips expose common manipulation techniques such as scapegoating, false dichotomies, and emotionally manipulative language, an approach the researchers call prebunking. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Inoculation Effect**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Inoculation Effect**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Inoculation Effect** work as an **epistemic-integrity review packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Inoculation Effect**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **Inoculation Effect** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

54.2.2.6 Lesson 6: Source-Agnostic Design: Effective Across Political Affiliations

Concept. Source-Agnostic Design: Effective Across Political Affiliations applies Agnostic, Design, Effective within Cognitive Security and Influence Resilience: learners use separate analysis of influence from persuasion design and information-integrity analysis and resilience education evidence before any judgment moves forward.

Why it matters. Source-Agnostic Design connects classroom vocabulary to Cognitive Security and Influence Resilience practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Source-Agnostic Design: Effective Across Political Affiliations rests on [152, 2026]. The most specific cited work observes: A University of Cambridge news article describing a large study, conducted with Bristol University and Google's Jigsaw, testing whether short animated videos can help people resist online manipulation. Use it for the working definition that **Source-Agnostic Design: Effective Across Political**

Affiliations can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Source-Agnostic Design**, reason from the sources cited in this row. [152, 2026] A University of Cambridge news article describing a large study, conducted with Bristol University and Google's Jigsaw, testing whether short animated videos can help people resist online manipulation. The 90-second clips expose common manipulation techniques such as scapegoating, false dichotomies, and emotionally manipulative language, an approach the researchers call prebunking. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Source-Agnostic Design**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must name the source descriptor, the bounded claim about **Source-Agnostic Design**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Source-Agnostic Design** work as an **epistemic-integrity review packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that Source-Agnostic Design: Effective Across Political Affiliations can be used while ignoring the rule to separate analysis of influence from persuasion design.

Transfer task. Transfer **Source-Agnostic Design** to a second module by preserving information-integrity analysis and resilience education, changing the source evidence, and naming a new reviewer.

54.2.2.7 Lesson 7: Scaling at $0.05 Per View; Campaign Applications

Concept. Scaling at $0.05 Per View; Campaign Applications applies Scaling, at, Per within Cognitive Security and Influence Resilience: learners use separate analysis of influence from persuasion design and information-integrity analysis and resilience education evidence before any judgment moves forward.

Why it matters. Scaling at $0.05 Per View; Campaign Applications matters in the **Cognitive Security and Influence Resilience** lane because information-integrity analysis and resilience education evidence must stay separate from judgment; counter-messaging as manipulation is a common failure.

Source support. Scaling at $0.05 Per View; Campaign Applications rests on [152, 2026]. The lead source's own note reads: A University of Cambridge news article describing a large study, conducted with Bristol University and Google's Jigsaw, testing whether short animated videos can help people resist online manipulation. Use it for fixing what **Scaling at $0.05 Per View; Campaign Applications** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Scaling at $0.05 Per View; Campaign Applications**, reason from the sources cited in this row. [152, 2026] A University of Cambridge news article describing a large study, conducted with Bristol University and Google's Jigsaw, testing whether short animated videos can help people resist online manipulation. The 90-second clips expose common manipulation techniques such as scapegoating, false dichotomies, and emotionally manipulative language, an approach the researchers call prebunking. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Scaling at $0.05 Per View; Campaign Applications**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must name the source descriptor, the bounded claim about **Scaling at 0 05 Per**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape this subject work as an **epistemic-integrity review packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that Scaling at $0.05 Per View; Campaign Applications is optional whenever separate analysis of influence from persuasion design feels inconvenient.

Transfer task. Transfer **Scaling at $0.05 Per View; Campaign Applications** to a second module by preserving information-integrity analysis and resilience education, changing the source evidence, and naming a new reviewer.

54.2.2.8 Lesson 8: Psychological Inoculation: Psychological inoculation and prebunking literacy

Concept. Psychological Inoculation: Psychological inoculation and prebunking literacy uses inoculation methods as evidence-informed, bounded, and context-dependent resilience education with transparent labels, source checks, non-manipulative corrections, and explicit measurement limits.

Why it matters. Psychological Inoculation connects classroom vocabulary to Cognitive Security and Influence Resilience practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Psychological Inoculation: Psychological inoculation and prebunking literacy rests on [184, 2026]. The closest source to this row notes: Sander van der Linden is Professor of Social Psychology in Society in the Department of Psychology. Use it for the claim that **Psychological Inoculation: Psychological inoculation and prebunking literacy** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Psychological Inoculation**, reason from the sources cited in this row. [184, 2026] Sander van der Linden is Professor of Social Psychology in Society in the Department of Psychology. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Psychological Inoculation**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Psychological Inoculation**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Psychological Inoculation** work as an **epistemic-integrity review packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Psychological Inoculation**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **Psychological Inoculation** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

54.2.2.9 Lesson 9: Inoculation to Resist Misinformation: Psychological inoculation and prebunking literacy

Concept. Inoculation to Resist Misinformation: Psychological inoculation and prebunking literacy analyzes influence campaigns through provenance, audience harm, attribution caution, and transparent response options.

Why it matters. Without explicit treatment of **Inoculation to Resist Misinformation**, treating resilience labels as permission to skip provenance review undermines information-integrity analysis and resilience education review; the lesson builds the habit to separate analysis of influence from persuasion design.

Source support. Inoculation to Resist Misinformation: Psychological inoculation and prebunking literacy rests on [185, 2026]. The most specific cited work observes: A 2024 JAMA Insights article by Sander van der Linden and Jon Roozenbeek on "inoculation" or prebunking as a psychological technique for resisting misinformation. Use it for the claim that **Inoculation to Resist Misinformation: Psychological inoculation and prebunking literacy** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Read **Inoculation to Resist Misinformation** against the works cited for this row. [185, 2026] A 2024 JAMA Insights article by Sander van der Linden and Jon Roozenbeek on "inoculation" or prebunking as a psychological technique for resisting misinformation. Part of the journal's Communicating Medicine series, it describes how preparing audiences in advance can build cognitive resistance to misleading narratives,

drawing an analogy to how vaccines build immunity. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Inoculation to Resist Misinformation**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Inoculation to Resist Misinformation**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Inoculation to Resist Misinformation** work as an **epistemic-integrity review packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Inoculation to Resist Misinformation**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Apply this module's safe boundary for **Inoculation to Resist Misinformation** to another artifact while keeping information-integrity analysis and resilience education and reviewer ownership explicit.

54.2.2.10 Lesson 10: Psychological inoculation evidence and boundary-condition

Concept. Psychological inoculation evidence and boundary-condition analyzes influence campaigns through provenance, audience harm, attribution caution, and transparent response options.

Why it matters. Without explicit treatment of **Psychological inoculation evidence**, treating resilience labels as permission to skip provenance review undermines information-integrity analysis and resilience education review; the lesson builds the habit to separate analysis of influence from persuasion design.

Source support. Psychological inoculation evidence and boundary-condition rests on [186, 2026]. The closest source to this row notes: Much like a viral contagion, misinformation can spread rapidly from one individual to another. Use it for the claim that **Psychological inoculation evidence and boundary-condition** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Psychological inoculation evidence**, reason from the sources cited in this row. [186, 2026] Much like a viral contagion, misinformation can spread rapidly from one individual to another. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. Build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Psychological inoculation evidence**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape this subject work as an **epistemic-integrity review packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Psychological inoculation evidence**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Apply this module's safe boundary for **Psychological inoculation evidence** to another artifact while keeping information-integrity analysis and resilience education and reviewer ownership explicit.

54.2.2.11 Lesson 11: NATO STRATCOM COE: Psychological inoculation and prebunking literacy

Concept. NATO STRATCOM COE: Psychological inoculation and prebunking literacy analyzes influence campaigns through provenance, audience harm, attribution caution, and transparent response options.

Why it matters. Without explicit treatment of **NATO STRATCOM COE**, treating resilience labels as permission to skip provenance review undermines information-integrity analysis and resilience education review; the lesson builds the habit to separate analysis of influence from persuasion design.

Source support. NATO STRATCOM COE: Psychological inoculation and prebunking literacy rests on [187, 2026]. The lead source's own note reads: A 2021 report published by the NATO Strategic Communications Centre of Excellence, authored by Jon Roozenbeek and Sander van der Linden of the Cambridge Social Decision-Making Lab, on inoculation theory and misinformation. Use it for fixing what **NATO STRATCOM COE: Psychological inoculation and prebunking literacy** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Read **NATO STRATCOM COE** against the works cited for this row. [187, 2026] A 2021 report published by the NATO Strategic Communications Centre of Excellence, authored by Jon Roozenbeek and Sander van der Linden of the Cambridge Social Decision-Making Lab, on inoculation theory and misinformation. It explores how psychology and behavioural science can help mitigate the spread of false and misleading information, noting that no single intervention through algorithms, legislation, or content moderation is sufficient. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **NATO STRATCOM COE**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **NATO STRATCOM COE**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **NATO STRATCOM COE** work as an **epistemic-integrity review packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **NATO STRATCOM COE**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **NATO STRATCOM COE** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

54.2.2.12 Lesson 12: Practical Guide to Prebunking: Psychological inoculation and prebunking literacy

Concept. Practical Guide to Prebunking: Psychological inoculation and prebunking literacy uses inoculation methods as evidence-informed, bounded, and context-dependent resilience education with transparent labels, source checks, non-manipulative corrections, and explicit measurement limits.

Why it matters. Practical Guide to Prebunking matters in the **Cognitive Security and Influence Resilience** lane because information-integrity analysis and resilience education evidence must stay separate from judgment; treating resilience labels as permission to skip provenance review is a common failure.

Source support. Practical Guide to Prebunking: Psychological inoculation and prebunking literacy rests on [151, 2026]. The most specific cited work observes: Grounded in inoculation theory, it describes how exposing people to weakened forms of manipulative content can help them develop resistance before they encounter it in the wild. Use it for the working definition that **Practical Guide to Prebunking: Psychological inoculation and prebunking literacy** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Practical Guide to Prebunking**, reason from the sources cited in this row. [151, 2026] A practitioner guide from Inoculation Science explaining prebunking as a proactive strategy to build preemptive resilience to misinformation. Grounded in inoculation theory, it describes how exposing people to weakened forms of manipulative content can help them develop resistance before they encounter it in the wild. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Practical Guide to Prebunking**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Practical Guide to Prebunking**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and

the reviewer accountable for correction. Shape **Practical Guide to Prebunking** work as an **epistemic-integrity review packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Practical Guide to Prebunking**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Apply this module's safe boundary for **Practical Guide to Prebunking** to another artifact while keeping information-integrity analysis and resilience education and reviewer ownership explicit.

54.2.2.13 Lesson 13: Critical Thinking Training vs. Misinformation: Systematic Review (Nature Comms, 2025)

Concept. Critical Thinking Training vs. Misinformation: Systematic Review (Nature Comms, 2025) analyzes influence campaigns through provenance, audience harm, attribution caution, and transparent response options.

Why it matters. Without explicit treatment of **Critical Thinking Training vs. Misinformation**, treating resilience labels as permission to skip provenance review undermines information-integrity analysis and resilience education review; the lesson builds the habit to separate analysis of influence from persuasion design.

Source support. Critical Thinking Training vs. Misinformation: Systematic Review (Nature Comms, 2025) rests on [181, 2026]. Its anchor reference records: Particularly noteworthy in this field is the resurgence of the cognitive inoculation theory. Use it for the claim that **Critical Thinking Training vs. Misinformation: Systematic Review (Nature Comms, 2025)** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Read **Critical Thinking Training vs. Misinformation** against the works cited for this row. [181, 2026] Particularly noteworthy in this field is the resurgence of the cognitive inoculation theory. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Critical Thinking Training vs. Misinformation**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Critical Thinking Training vs Misinformation**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Critical Thinking Training vs. Misinformation** work as an **epistemic-integrity review packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Critical Thinking Training vs. Misinformation**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Transfer **Critical Thinking Training vs. Misinformation** from this module to a second motif by preserving information-integrity analysis and resilience education, replacing action with audit, and naming the blocked use.

54.2.2.14 Lesson 14: Transparent prebunking education and review workflow

Concept. Transparent prebunking education and review workflow uses inoculation methods as evidence-informed, bounded, and context-dependent resilience education with transparent labels, source checks, non-manipulative corrections, and explicit measurement limits.

Why it matters. Analysts use **Transparent prebunking education** to separate analysis of influence from persuasion design. A defensible treatment names the judgment it enables for information-integrity analysis and resilience education review, the proof limit that treating resilience labels as permission to skip provenance review would otherwise hide, and the reviewer accountable for challenge.

Source support. Transparent prebunking education and review workflow rests on [308, 2026] and [311, 2026]. The closest source to this row notes: It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering. Use them for fixing what **Transparent prebunking education and review workflow** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Read **Transparent prebunking education** against the works cited for this row. [308, 2026] An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure. [311, 2026] An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Transparent prebunking education**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Transparent prebunking education and review**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Transparent prebunking education** work as an **epistemic-integrity review packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Transparent prebunking education**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Apply this module's safe boundary for **Transparent prebunking education** to another artifact while keeping information-integrity analysis and resilience education and reviewer ownership explicit.

54.2.3 Psychological Inoculation and Prebunking worked safe example: synthetic inputs, evidence, and review

Worked example: a sample public-library class evaluates a synthetic rumor about a community service and compares transparent correction options. [242, 2026]; [243, 2026].

Triangulation anchors. In module 39's worked-example section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **cognitive resilience and epistemic integrity**. Learners use a **epistemic-integrity review packet** and keep this boundary visible: No manipulation, covert persuasion, medicalized claims, or population-level targeting.

Frame. The classroom question centers on **Psychological inoculation and prebunking literacy**. Excluded actions stay explicit, and the **Cognitive-Resilience Lens** planning question is: How does the module protect autonomy, attention, trust, and decision quality without designing persuasion?

Inputs. For the **Psychological inoculation and prebunking literacy** scenario, use sample posts, source timestamps, public-service facts, and a media-literacy rubric. The Cognitive-Resilience Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Psychological inoculation and prebunking literacy**, students trace narrative provenance, separate observation from attribution, name audience harms, and design a transparent lesson. Pause whenever an inference about Psychological inoculation and prebunking literacy appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Psychological inoculation and prebunking literacy** classroom scenario; unit artifact = epistemic-integrity review packet; evidence = allowed inputs; method = information-integrity analysis and resilience education; output = a narrative-risk map with caveats, response options, and no microtargeted persuasion; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Psychological inoculation and prebunking literacy** as "Cognitive-Resilience Lens confirms it" is not enough. The revision ties the claim to information-integrity analysis and resilience education, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Psychological inoculation and prebunking literacy** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

54.2.4 Psychological Inoculation and Prebunking practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Cognitive-Resilience Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**.

Triangulation anchors. In module 39's practice-sequence section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Psychological inoculation and prebunking literacy, Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy, Prebunking Interventions Based on Inoculation: Psychological inoculation and prebunking literacy; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Cognitive Security and Influence Resilience** lane.
2. Frame	Answer the lens question: How does the module protect autonomy, attention, trust, and decision quality without designing persuasion?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Psychological inoculation and prebunking literacy: narrative-risk map with provenance, uncertainty, audience harms, and response options.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the epistemic-integrity review packet fields for Psychological inoculation and prebunking literacy.	Unit profile note.	Evidence artifacts include provenance chain, correction option.
4. Challenge	Test the misconception that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.	Failure-mode note.	The artifact applies the key distinction: separate analysis of influence from persuasion design.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

54.2.4.1 Psychological Inoculation and Prebunking instructor notes: source reasoning, review points, and studio focus

Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**. [242, 2026]; [243, 2026].

54.2.4.2 Psychological Inoculation and Prebunking extension exercise: peer validation and refresh trigger review

Evidence anchor. Section 54; [242, 2026].

Have learners swap artifacts and apply the **Cognitive-Resilience Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**.

54.2.5 Psychological Inoculation and Prebunking knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 54; [242, 2026].

1. Explain how **Psychological inoculation and prebunking literacy** is defined here; name the source descriptor that supports the definition.
2. Contrast **Psychological inoculation and prebunking literacy** with **Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy** using the **Cognitive-Resilience Lens** artifact fields.
3. Identify one failure mode from the **Cognitive Security and Influence Resilience** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which response informs people without crossing into MISO-style manipulation or unverified attribution?
5. Correct this misconception: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

54.2.5.1 Psychological Inoculation and Prebunking answer quality rubric: source evidence, uncertainty, and safe transfer

Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Psychological inoculation and prebunking literacy** without source evidence, uncertainty, or a safe transfer task.

54.3 Psychological Inoculation and Prebunking assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 54; [242, 2026].

54.3.1 Psychological Inoculation and Prebunking evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 54; [242, 2026].

54.3.2 Psychological Inoculation and Prebunking transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 54; [242, 2026].

54.3.2.1 Psychological Inoculation and Prebunking lineage and source tradition: profile, concepts, and first anchors This sits in the **Cognitive Security and Influence Resilience** lineage: protecting attention, belief formation, and decision quality without turning resilience education into manipulation. [242, 2026]; [243, 2026].

54.3.2.2 Psychological Inoculation and Prebunking working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 54; [242, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**, with provenance and reviewability throughout.

54.3.2.3 Psychological Inoculation and Prebunking knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [242, 2026]; [243, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

54.3.2.4 Psychological Inoculation and Prebunking transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 54; [242, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**.
- **Evidence contract:** keep the **Cognitive Security and Influence Resilience** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

54.3.2.5 Psychological Inoculation and Prebunking profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 54; [242, 2026].

The matched profile emphasizes protecting attention, belief formation, and decision quality without turning resilience education into manipulation. The method stack is claim decomposition, narrative provenance, inoculation framing, bias checks, audience-risk review, and after-action learning; the local topic cluster is **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**.

54.3.3 Psychological Inoculation and Prebunking evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 54; [242, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Cognitive Security and Influence Resilience** profile tells reviewers what evidence is strong enough for the module artifact built around **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**.

54.3.3.1 Psychological Inoculation and Prebunking guide source spine: inherited keys and local citation roles Primary guide citations: [242, 2026]; [243, 2026]; [245, 2026]; [279, 2026]; [282, 2026]; [284, 2026]; [289, 2026]; [291, 2026]; [296, 2026]; [181, 2026]; [182, 2026]; [183, 2026]; [152, 2026]; [184, 2026]; [185, 2026]; [186, 2026]; [187, 2026]; [151, 2026]; [308, 2026]; [311, 2026].

54.3.3.2 Psychological Inoculation and Prebunking verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [242, 2026]; [243, 2026].

Tier	What counts	How it is used
Source guide	[242, 2026]; [243, 2026]; [245, 2026]; [279, 2026]; [282, 2026]; [284, 2026]; [289, 2026]; [291, 2026]; [296, 2026]; [181, 2026]; [182, 2026]; [183, 2026]; [152, 2026]; [184, 2026]; [185, 2026]; [186, 2026]; [187, 2026]; [151, 2026]; [308, 2026]; [311, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 39's source-canon section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy** and [242, 2026]; [243, 2026], but only directly verified source URLs are encoded as citations.

54.3.3.3 Psychological Inoculation and Prebunking intelligence practice lens: evidence artifact and safety check Practice lens: **Cognitive-Resilience Lens** for **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**. [242, 2026]; [243, 2026].

Planning question: How does the module protect autonomy, attention, trust, and decision quality without designing persuasion?

Evidence artifact: narrative-risk map with provenance, uncertainty, audience harms, and response options.

Validation rule: distinguish observation, attribution, impact assessment, and resilience response. Applied to **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**.

Handoff contract: handoff supports transparency, education, and resilience, not microtargeted influence or deception.

Safety check: exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning.

54.3.3.4 Psychological Inoculation and Prebunking runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 54; [242, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	39.99	39.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Psychological Inoculation and Prebunking to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Bounded autonomy, procurement, incident-response, and assurance studio	39.101	39.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Psychological Inoculation and Prebunking	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Model-card, recoverability, retention, and learner-support evidence package	39.102	39.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Psychological Inoculation and Prebunking	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Psychological inoculation and prebunking literacy	39.1	39.1 source title transformed into safe curriculum treatment; original: Inoculation Theory: McGuire and Papageorgis (1961) to Present	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Psychological inoculation and prebunking literacy	39.2	39.2 source title transformed into safe curriculum treatment; original: Psychological Inoculation Against Misinformation: Meta-Analysis	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Psychological inoculation and prebunking literacy	39.3	39.3 source title transformed into safe curriculum treatment; original: Prebunking Interventions Based on Inoculation Theory (Harvard Kennedy School)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Cambridge/Jigsaw YouTube Field Study: 5.4 Million Users, 7 Experiments	39.4	39.4 Cambridge/Jigsaw YouTube Field Study: 5.4 Million Users, 7 Experiments	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Psychological inoculation and prebunking literacy	39.4.1	39.4.1 source title transformed into safe curriculum treatment; original: Inoculation Effect: Measured Improvement in Manipulation Recognition	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Source-Agnostic Design: Effective Across Political Affiliations	39.4.2	39.4.2 Source-Agnostic Design: Effective Across Political Affiliations	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Scaling at $0.05 Per View; Campaign Applications	39.4.3	39.4.3 Scaling at $0.05 Per View; Campaign Applications	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Psychological inoculation and prebunking literacy	39.5	39.5 source title transformed into safe curriculum treatment; original: Psychological Inoculation (JNNP, van der Linden 2023)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Psychological inoculation and prebunking literacy	39.6	39.6 source title transformed into safe curriculum treatment; original: “Inoculation” to Resist Misinformation (JAMA, 2024)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Psychological inoculation evidence and boundary-condition	39.7	39.7 source title transformed into safe curriculum treatment; original: Psychological Inoculation Against Misinformation: Current Evidence and Boundary Conditions (ANNALS, 2022)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Psychological inoculation and prebunking literacy	39.8	39.8 source title transformed into safe curriculum treatment; original: NATO STRATCOM COE: Inoculation Theory and Misinformation (PDF)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Psychological inoculation and prebunking literacy	39.9	39.9 source title transformed into safe curriculum treatment; original: A Practical Guide to Prebunking (Cambridge/Jigsaw/BBC)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Critical Thinking Training vs. Misinformation: Systematic Review (Nature Comms, 2025)	39.10	39.10 Critical Thinking Training vs. Misinformation: Systematic Review (Nature Comms, 2025)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Transparent prebunking education and review workflow	39.11	39.11 source title transformed into safe curriculum treatment; original: Operationalizing Prebunking in AGEINT: Transparent Resilience Education and	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning

54.3.3.5 Psychological Inoculation and Prebunking reusable subsection contract: topic rows, artifacts, and safety duties Evidence anchor. Section 54; [242, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Psychological inoculation and prebunking literacy	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Prebunking Interventions Based on Inoculation: Psychological inoculation and prebunking literacy	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Cambridge/Jigsaw YouTube Field Study: 5.4 Million Users, 7 Experiments	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Inoculation Effect: Psychological inoculation and prebunking literacy	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Source-Agnostic Design: Effective Across Political Affiliations	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Scaling at $0.05 Per View; Campaign Applications	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Psychological Inoculation: Psychological inoculation and prebunking literacy	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Inoculation to Resist Misinformation: Psychological inoculation and prebunking literacy	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Psychological inoculation evidence and boundary-condition	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
NATO STRATCOM COE: Psychological inoculation and prebunking literacy	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Practical Guide to Prebunking: Psychological inoculation and prebunking literacy	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Critical Thinking Training vs. Misinformation: Systematic Review (Nature Comms, 2025)	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Transparent prebunking education and review workflow	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning

54.3.3.6 Psychological Inoculation and Prebunking annotated source ledger: real titles and local contribution Each source cited by this **Cognitive Security and Influence Resilience** module is paired below with its real title and a one-line note on what it contributes to **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**.

Source	Cited work	What it contributes	Status
[242, 2026]	Guidance for Generative AI in Education and Research	Official UNESCO generative AI education guidance.	original source-guide
[243, 2026]	AI Competency Frameworks for Teachers and Students	A UNESCO announcement of two new AI competency frameworks, one for students and one for teachers, intended to guide safe and responsible engagement with artificial intelligence in education. The student framework emphasizes a human-centered perspective, ethical use, foundational AI knowledge, and design thinking, while the teacher framework covers ethics, technical understanding, and pedagogy.	verified source-guide
[245, 2026]	Artificial Intelligence in Education	Official OECD AI in education topic page.	original source-guide
[279, 2026]	Open Contracting Data Standard	The documentation homepage for the Open Contracting Data Standard, version 1.1.5, maintained by the Open Contracting Partnership to support disclosure of government contracting data across the procurement lifecycle. It provides a common data model spanning planning, tender, award, contract, and implementation stages, along with a primer, implementation guidance, technical schemas, and validation tooling.	verified source-guide
[282, 2026]	AI Research: Security and Resilience	A NIST page on AI research focused on security and resilience, framing these as core characteristics of trustworthy AI under the NIST AI Risk Management Framework.	verified source-guide
[284, 2026]	Verifiable Credential Data Integrity 1.0	The W3C Recommendation for Verifiable Credential Data Integrity 1.0, published May 2025, defining mechanisms for ensuring the authenticity and integrity of verifiable credentials using cryptographic proofs. It specifies a process of data transformation, hashing, and proof generation, and a corresponding verification procedure, along with a proof data model containing properties such as type, verification method, purpose, and proof value.	verified source-guide
[289, 2026]	Guidance for Organisations Using the Algorithmic Transparency Recording Standard	This is a GOV.UK guidance page published by the Government Digital Service that instructs public sector organizations on completing the Algorithmic Transparency Recording Standard (ATRS) template and publishing their records to the GOV.UK repository. It applies both to central government bodies required to publish under mandatory policy and to other public sector bodies doing so voluntarily.	verified source-guide

Source	Cited work	What it contributes	Status
[291, 2026]	Revised 508 Standards and 255 Guidelines	Official documentation from the U.S. Access Board on the Revised 508 Standards and 255 Guidelines for information and communication technology accessibility. It establishes mandatory accessibility requirements for federal agencies and voluntary guidelines for telecommunications manufacturers, covering hardware, software, websites, electronic documents, and support services.	verified source-guide
[296, 2026]	Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile	NIST AI 600-1, the Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, a cross-sectoral companion resource to the NIST AI RMF 1.0 issued pursuant to Executive Order 14110. It identifies risks that are unique to or amplified by generative AI and organizes suggested actions for managing those risks, mapped to the AI RMF functions.	verified source-guide
[181, 2026]	Effectiveness of training actions aimed at improving critical thinking	Particularly noteworthy in this field is the resurgence of the cognitive inoculation theory.	original source-guide
[182, 2026]	Psychological Inoculation for Credibility Assessment, Sharing	A 2023 meta-analysis in the Journal of Medical Internet Research evaluating psychological inoculation, or prebunking, as a strategy against misinformation, drawing on 42 studies with over 42,000 participants. It reports bounded improvements in people's ability to distinguish misinformation from real information, while finding limited effect on intentions to share misinformation and leaving context, durability, and transfer conditions for review.	verified source-guide
[183, 2026]	Prebunking interventions based on "inoculation" theory can reduce	A 2020 peer-reviewed study in the Harvard Kennedy School Misinformation Review by Roozenbeek, van der Linden, and Nygren testing the Bad News game as a prebunking intervention grounded in inoculation theory. Players take the role of a misinformation creator to learn common manipulation techniques such as impersonation, emotional appeals, polarization, and conspiratorial framing, building resistance to deceptive content.	verified source-guide
[152, 2026]	Social media experiment reveals potential to 'inoculate' millions	A University of Cambridge news article describing a large study, conducted with Bristol University and Google's Jigsaw, testing whether short animated videos can help people resist online manipulation. The 90-second clips expose common manipulation techniques such as scapegoating, false dichotomies, and emotionally manipulative language, an approach the researchers call prebunking.	verified source-guide
[184, 2026]	Psychological inoculation against misinformation	Sander van der Linden is Professor of Social Psychology in Society in the Department of Psychology.	original source-guide

Source	Cited work	What it contributes	Status
[185, 2026]	"Inoculation" to Resist Misinformation - PubMed	A 2024 JAMA Insights article by Sander van der Linden and Jon Roozenbeek on "inoculation" or prebunking as a psychological technique for resisting misinformation. Part of the journal's Communicating Medicine series, it describes how preparing audiences in advance can build cognitive resistance to misleading narratives, drawing an analogy to how vaccines build immunity.	verified source-guide
[186, 2026]	Psychological Inoculation against Misinformation: Current Evidence and Future Directions - Cecilie S. Traberg, Jon Roozenbeek, Sander van der Linden, 2022	Much like a viral contagion, misinformation can spread rapidly from one individual to another.	original source-guide
[187, 2026]	INOCULATION THEORY AND MISINFORMATION	A 2021 report published by the NATO Strategic Communications Centre of Excellence, authored by Jon Roozenbeek and Sander van der Linden of the Cambridge Social Decision-Making Lab, on inoculation theory and misinformation. It explores how psychology and behavioural science can help mitigate the spread of false and misleading information, noting that no single intervention through algorithms, legislation, or content moderation is sufficient.	verified source-guide
[151, 2026]	A Practical Guide to Prebunking Misinformation - Inoculation Science	A practitioner guide from Inoculation Science explaining prebunking as a proactive strategy to build preemptive resilience to misinformation. Grounded in inoculation theory, it describes how exposing people to weakened forms of manipulative content can help them develop resistance before they encounter it in the wild.	verified source-guide
[308, 2026]	Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure	An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure.	verified source-guide
[311, 2026]	Countering Information Threats	An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering.	verified source-guide

Where this sits. This module's overview is Section 54; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

54.3.4 Psychological Inoculation and Prebunking governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 54; [242, 2026].

54.3.5 Psychological Inoculation and Prebunking analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 39's governance-boundary section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **Cognitive Security and Influence Resilience** for **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**. [242, 2026]; [243, 2026].

Curriculum topic spine: Psychological inoculation and prebunking literacy, **Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**, **Prebunking Interventions Based on Inoculation: Psychological inoculation and prebunking literacy**. **Verified anchor cluster:** [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]; [OECD, 2026c]; [for Security Policy, 2025]; [Community, 2020a].

Conceptual depth: protecting attention, belief formation, and decision quality without turning resilience education into manipulation.

Method stack: claim decomposition, narrative provenance, inoculation framing, bias checks, audience-risk review, and after-action learning.

Composability contract: separate descriptive analysis, normative assessment, response options, and protected-audience considerations.

Known failure modes: counter-messaging as manipulation, overclaiming intent, pathologizing audiences, and collapsing uncertainty into moral certainty.

Defensive boundary: practice uses benign simulations and resilience education; it does not create persuasion campaigns, impersonation, or deception plans. Applied to **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**.

Anchor	Why it matters here
[Cybersecurity and Agency, 2024b]	Official CISA guidance on foreign influence operations targeting critical infrastructure. Checked as of 2026-05-21; role: source_quality_anchor.
[Organization, 2026b]	Official NATO counter-information-threat guidance. Checked as of 2026-05-21; role: source_quality_anchor.
[Cybersecurity and Agency, 2026b]	Official CISA election-security source for public-resilience, foreign-influence awareness, rumor control, and defensive communication framing. Checked as of 2026-05-21; role: curriculum_anchor.
[Organization, 2026c]	Official NATO source for hybrid-threat resilience across cyber, information, economic, political, and military pressure. Checked as of 2026-05-21; role: curriculum_anchor.
[OECD, 2026c]	Official OECD policy source for information integrity, governance responses, public trust, and democratic resilience. Checked as of 2026-05-21; role: curriculum_anchor.
[for Security Policy, 2025]	Policy-scholarship source for cognitive security, information literacy, critical thinking, and whole-of-society resilience. Checked as of 2026-05-21; role: curriculum_anchor.
[Community, 2020a]	Official IC framework for AI goals, authorities, human judgment, bias mitigation, testing, documentation, explainability, and review. Checked as of 2026-05-21; role: curriculum_anchor.

54.3.5.1 Psychological Inoculation and Prebunking evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **Cognitive Security and Influence Resilience** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [242, 2026]; [243, 2026].

54.3.6 Psychological Inoculation and Prebunking agentic boundary: assist, approve, block, and record

Evidence anchor. Section 54; [242, 2026].

AGEINT translation is bounded by the **Cognitive Security and Influence Resilience** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**.

54.3.6.1 Psychological Inoculation and Prebunking permitted defensive utility: curriculum uses and safe outputs

Evidence anchor. Section 54; [242, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**.

54.3.6.2 Psychological Inoculation and Prebunking excluded operational boundary: blocked actions and stop rules

Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [242, 2026]; [243, 2026] and **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

54.3.7 Psychological Inoculation and Prebunking governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 54; [242, 2026].

Governance is practiced as a gate on the **Cognitive Security and Influence Resilience** lane. Learners use the **Cognitive-Resilience Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**.

54.3.7.1 Psychological Inoculation and Prebunking governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [242, 2026]; [243, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Cognitive Security and Influence Resilience** failure modes and the **Cognitive-Resilience Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

54.3.7.2 Psychological Inoculation and Prebunking evidence package handoff: appendices, records, and reuse

Evidence anchor. Section 54; [242, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Cognitive-Resilience Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**.

54.3.7.3 Psychological Inoculation and Prebunking current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**. [242, 2026]; [243, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_cisa_foreign_influence` for **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**?	Preparing for and Mitigating Foreign Influence Operations; lane `source_quality_spine`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official CISA guidance on foreign influence operations targeting critical infrastructure.
What does the module inherit from `official_nato_counter_information_threats` for **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**?	Countering Information Threats; lane `source_quality_spine`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official NATO counter-information-threat guidance.
What does the module inherit from `official_cisa_election_security_influence` for **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**?	Election Security; lane `cognitive_influence_security`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official CISA election-security source for public-resilience, foreign-influence awareness, rumor control, and defensive communication framing.
What does the module inherit from `official_nato_hybrid_threats` for **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**?	Countering Hybrid Threats; lane `cognitive_influence_security`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official NATO source for hybrid-threat resilience across cyber, information, economic, political, and military pressure.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 54; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

54.3.8 Psychological Inoculation and Prebunking assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 54; [242, 2026].

54.3.9 Psychological Inoculation and Prebunking assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 54; [242, 2026].

54.3.9.1 Psychological Inoculation and Prebunking capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**.
Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy** and [242, 2026]; [243, 2026].

54.3.9.2 Psychological Inoculation and Prebunking instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy** and [242, 2026]; [243, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

54.3.9.3 Psychological Inoculation and Prebunking assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Psychological inoculation and prebunking literacy	Completed **narrative-risk map with provenance, uncertainty, audience harms, and response options** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy	Completed **narrative-risk map with provenance, uncertainty, audience harms, and response options** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Prebunking Interventions Based on Inoculation: Psychological inoculation and prebunking literacy	Completed **narrative-risk map with provenance, uncertainty, audience harms, and response options** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

54.3.10 Psychological Inoculation and Prebunking refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [242, 2026]; [243, 2026] and **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**.

54.3.10.1 Psychological Inoculation and Prebunking refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**. The local signals begin with [242, 2026]; [243, 2026].

54.3.10.2 Psychological Inoculation and Prebunking claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**, and the source spine for these checks begins with [242, 2026]; [243, 2026].

54.3.11 Psychological Inoculation and Prebunking reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [242, 2026]; [243, 2026].
Triangulation anchors. In module 39's review-checklist section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy**. [242, 2026]; [243, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.

- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

54.3.12 Psychological Inoculation and Prebunking learning-path links: module map, overview, and curriculum atlas

Use the cross-links below to place **Psychological inoculation and prebunking literacy; Psychological Inoculation Against Misinformation: Psychological inoculation and prebunking literacy** in the wider unit: the orientation sets the frame, the parent unit supplies the shared safety posture, and the neighbouring modules show what evidence enters and leaves. Lead sources: [242, 2026]; [243, 2026].

Section 2, Section 51, Section 53, Section 55

55 Cognitive Security Operations

55.0.1 Cognitive Security Operations figures and course links: visual evidence, source flow, and navigation

The module uses Figure 115 and Figure 107 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 51, Section 54, Section 56.
This module teaches the **Cognitive Security and Influence Resilience** lane through a bounded, source-backed coursebook chapter. [238, 2026]; [239, 2026].

55.1 Cognitive Security and Influence Resilience frame for Cognitive Security Operations: source context, topic focus, and reader task

Evidence anchor. Section 55; [238, 2026].

55.1.1 Cognitive Security Operations orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 55; [238, 2026].

55.1.2 Cognitive Security Operations conceptual primer: source context, core model, and reader task

This chapter teaches cognitive security as protection of attention, trust, memory, and decision quality without creating manipulation. The chapter uses **Cognitive-Resilience Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**.
The central distinction is to separate analysis of influence from persuasion design. Core topics include **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials; Deepfakes, Voice Cloning, and Digital Identity Attacks**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [238, 2026]; [239, 2026].
Learners move from vocabulary and the **Cognitive-Resilience Lens** distinction through topic lessons on **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making** with evidence and misconception checks, then assemble a **narrative-risk map with provenance, uncertainty, audience harms, and response options** with safety and rights gates.

55.1.3 Cognitive Security Operations learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 55; [238, 2026].

- Connect **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making and Cognitive influence-analysis case review using sample materials** to **Cognitive Security and Influence Resilience** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate analysis of influence from persuasion design; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as counter-messaging as manipulation, overclaiming intent, pathologizing audiences, and collapsing uncertainty into moral certainty, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: practice uses benign simulations and resilience education; it does not create persuasion campaigns, impersonation, or deception plans.

55.1.4 Cognitive Security Operations core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 55; [238, 2026].

Term	Working definition
Narrative provenance	where a claim, frame, or story came from and how it spread
Prebunking	transparent education that helps people recognize misleading patterns before exposure
Audience harm	a privacy, dignity, autonomy, or trust risk for people receiving information
Attribution caution	the rule that intent and origin claims need strong evidence
Resilience response	a transparent education, correction, or process improvement that avoids manipulation
MISO boundary	the line between accountable public messaging analysis and covert influence design
Inoculation	building recognition of manipulation tactics without deploying persuasion against a population
The Cognitive Attack Surface: Attention,...	Key terms: Cognitive, Attack, Surface.
Cognitive influence-analysis case review using...	Key terms: Cognitive, influence, analysis.

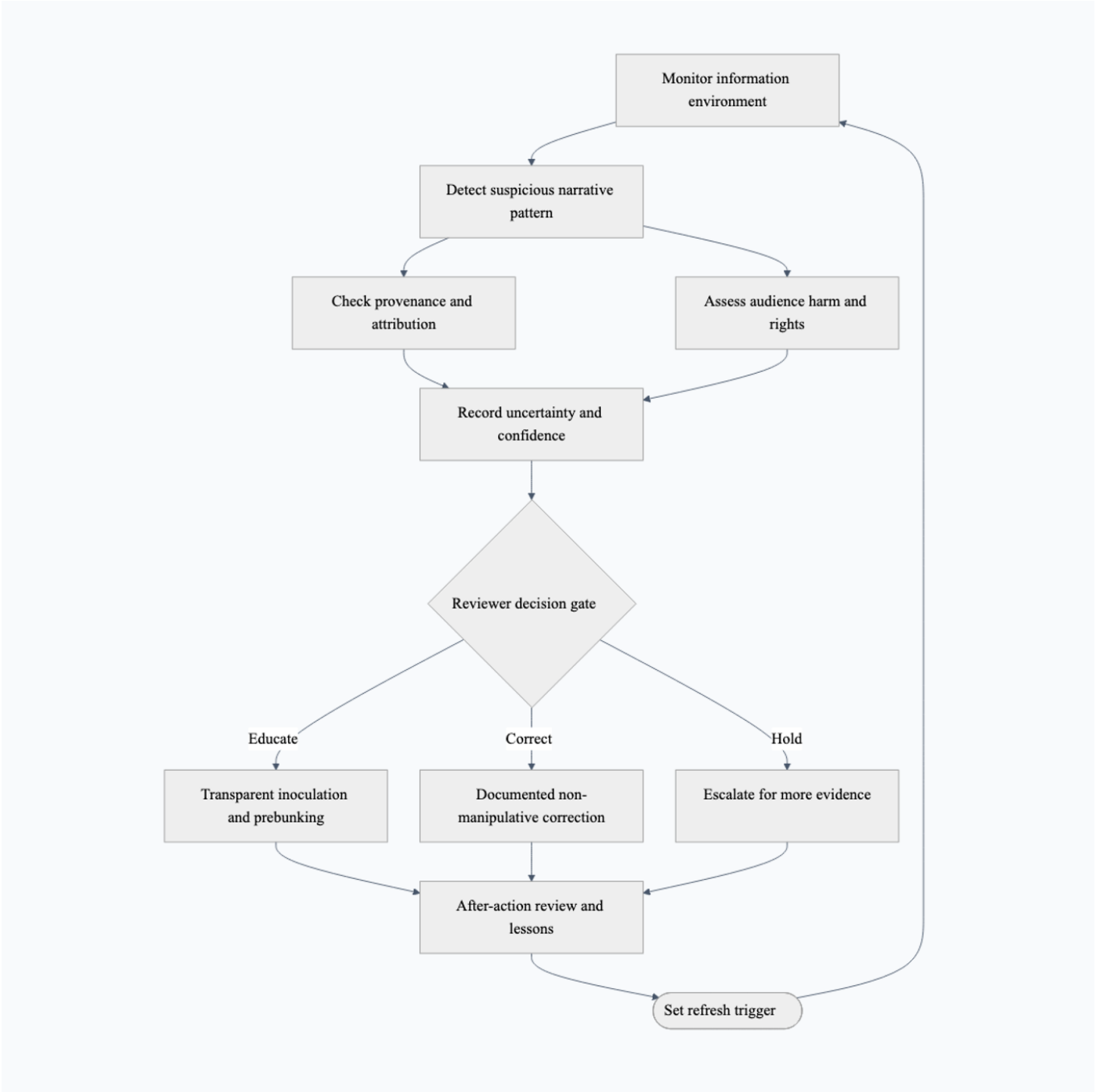


Figure 115: A defensive cycle for protecting attention, trust, and decision quality through monitoring, transparent education, and reviewed correction. In the cognitive security / cognitive security operations section, it lets readers compare Monitor information environment, Detect suspicious narrative pattern, Check provenance and attribution, and Assess audience harm and rights so the visual functions as a traceable course aid rather than an unscoped assertion.

55.2 Cognitive-Resilience Lens path for Cognitive Security Operations: lesson cluster, safe artifact, and review

Evidence anchor. Section 55; [238, 2026].

55.2.1 Cognitive Security Operations practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 55; [238, 2026].

55.2.2 Cognitive Security Operations topic lessons: source-backed concepts and transfer tasks

This module builds cognitive security as protection of attention, trust, memory, and decision quality without creating manipulation. The sequence opens with **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making**, **Cognitive influence-analysis case review using sample materials**, **Deepfakes, Voice Cloning, and Digital Identity Attacks** and applies the **Cognitive-Resilience Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 107; module overview Section 55; curriculum atlas Section 2.

Triangulation anchors. In module 40's topic-lessons section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

55.2.2.1 Lesson 1: The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making

Concept. The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making maps cognitive attack surfaces: attention, belief formation, narrative provenance, and transparent correction options.

Why it matters. Analysts use **The Cognitive Attack Surface** to separate analysis of influence from persuasion design. A defensible treatment names the judgment it enables for information-integrity analysis and resilience education review, the proof limit that treating resilience labels as permission to skip provenance review would otherwise hide, and the reviewer accountable for challenge.

Source support. The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making rests on [095, 2026]. The most specific cited work observes: This policy paper examines the emergence of cognitive security. Use it for the claim that **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Ground **The Cognitive Attack Surface** in the evidence the row cites. [095, 2026] This policy paper examines the emergence of cognitive security. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **The Cognitive Attack Surface**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Cognitive Attack Surface**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **The Cognitive Attack Surface** work as an **epistemic-integrity review packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **The Cognitive Attack Surface**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Transfer **The Cognitive Attack Surface** from this module to a second motif by preserving information-integrity analysis and resilience education, replacing action with audit, and naming the blocked use.

55.2.2.2 Lesson 2: Cognitive influence-analysis case review using sample materials

Concept. Cognitive influence-analysis case review using sample materials studies influence doctrine as audience analysis, message integrity, and ethics—not as manipulation technique.

Why it matters. Without explicit treatment of **Cognitive influence-analysis case review**, treating resilience labels as permission to skip provenance review undermines information-integrity analysis and resilience education review; the lesson builds the habit to separate analysis of influence from persuasion design.

Source support. Cognitive influence-analysis case review using sample materials rests on [105, 2026]. Its anchor reference records: The paper argues that AI-powered computational propaganda poses national security threats that existing ethical frameworks do not address, and proposes 'cognitive security' as a productive conceptual lens for evaluating the ethics of automated influence operations and potential defensive responses. Use it for pinning down the scope of **Cognitive influence-analysis case review using sample materials**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Cognitive influence-analysis case review**, reason from the sources cited in this row. [105, 2026] Sarah Rajtmajer and Daniel Susser, 'Automated Influence and the Challenge of Cognitive Security,' in Hot Topics in the Science of Security (HotSoS '20), April 2020, ACM. The paper argues that AI-powered computational propaganda poses national security threats that existing ethical frameworks do not address, and proposes 'cognitive security' as a productive conceptual lens for evaluating the ethics of automated influence operations and potential defensive responses. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Cognitive influence-analysis case review**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Cognitive influence-analysis case review using**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Cognitive influence-analysis case review** work as an **epistemic-integrity review packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Cognitive influence-analysis case review**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Transfer **Cognitive influence-analysis case review** from this module to a second motif by preserving information-integrity analysis and resilience education, replacing action with audit, and naming the blocked use.

55.2.2.3 Lesson 3: Deepfakes, Voice Cloning, and Digital Identity Attacks

Concept. Deepfakes, Voice Cloning, and Digital Identity Attacks focuses on transparent resilience education: provenance, audience harm, attribution caution, and non-manipulative response options.

Why it matters. Deepfakes, Voice Cloning, and Digital Identity Attacks connects classroom vocabulary to Cognitive Security and Influence Resilience practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Deepfakes, Voice Cloning, and Digital Identity Attacks rests on [300, 2026], [304, 2026], and [306, 2026]. The most specific cited work observes: NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Use them for pinning down the scope of **Deepfakes, Voice Cloning, and Digital Identity Attacks**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Read **Deepfakes, Voice Cloning, and Digital Identity Attacks** against the works cited for this row. [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Deepfakes, Voice Cloning, and Digital Identity Attacks**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Deepfakes Voice Cloning and Digital**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape this subject work as an **epistemic-integrity review packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Deepfakes, Voice Cloning, and Digital Identity Attacks**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **Deepfakes, Voice Cloning, and Digital Identity Attacks** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

55.2.2.4 Lesson 4: From Spycraft to Self-Mastery: SATs for Personal Cognitive Security

Concept. From Spycraft to Self-Mastery: SATs for Personal Cognitive Security maps cognitive attack surfaces: attention, belief formation, narrative provenance, and transparent correction options.

Why it matters. From Spycraft to Self-Mastery matters in the **Cognitive Security and Influence Resilience** lane because information-integrity analysis and resilience education evidence must stay separate from judgment; treating resilience labels as permission to skip provenance review is a common failure.

Source support. From Spycraft to Self-Mastery: SATs for Personal Cognitive Security rests on [188, 2026]. Its anchor reference records: An article on Spotter Up by Eugene Nielsen arguing that structured analytic techniques (SATs) developed for intelligence analysis can improve everyday decision-making. Use it for the claim that **From Spycraft to Self-Mastery: SATs for Personal Cognitive Security** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Read **From Spycraft to Self-Mastery** against the works cited for this row. [188, 2026] An article on Spotter Up by Eugene Nielsen arguing that structured analytic techniques (SATs) developed for intelligence analysis can improve everyday decision-making. It describes cognitive biases such as confirmation bias and overconfidence, then outlines categories of SATs including diagnostic, contrarian, imaginative, structuring, and decision-support methods. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **From Spycraft to Self-Mastery**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Spycraft to Self-Mastery**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **From Spycraft to Self-Mastery** work as an **epistemic-integrity review packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **From Spycraft to Self-Mastery**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Apply this module's safe boundary for **From Spycraft to Self-Mastery** to another artifact while keeping information-integrity analysis and resilience education and reviewer ownership explicit.

55.2.2.5 Lesson 5: Building Organizational Cognitive Resilience

Concept. Building Organizational Cognitive Resilience focuses on transparent resilience education: provenance, audience harm, attribution caution, and non-manipulative response options.

Why it matters. Building Organizational Cognitive Resilience connects classroom vocabulary to Cognitive Security and Influence Resilience practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Building Organizational Cognitive Resilience rests on [095, 2026]. The lead source's own note reads: This policy paper examines the emergence of cognitive security. Use it for fixing what **Building Organizational Cognitive Resilience** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Read **Building Organizational Cognitive Resilience** against the works cited for this row. [095, 2026] This policy paper examines the emergence of cognitive security. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. Build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Building Organizational Cognitive Resilience**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape this subject work as an **epistemic-integrity review packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Building Organizational Cognitive Resilience**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **Building Organizational Cognitive Resilience** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

55.2.2.6 Lesson 6: National Cognitive Security Centers: Policy Proposals

Concept. National Cognitive Security Centers: Policy Proposals maps cognitive attack surfaces: attention, belief formation, narrative provenance, and transparent correction options.

Why it matters. Without explicit treatment of **National Cognitive Security Centers**, treating resilience labels as permission to skip provenance review undermines information-integrity analysis and resilience education review; the lesson builds the habit to separate analysis of influence from persuasion design.

Source support. National Cognitive Security Centers: Policy Proposals rests on [095, 2026]. The most specific cited work observes: This policy paper examines the emergence of cognitive security. Use it for the working definition that **National Cognitive Security Centers: Policy Proposals** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Ground **National Cognitive Security Centers** in the evidence the row cites. [095, 2026] This policy paper examines the emergence of cognitive security. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **National Cognitive Security Centers**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **National Cognitive Security Centers**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and

the reviewer accountable for correction. Shape **National Cognitive Security Centers** work as an **epistemic-integrity review packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **National Cognitive Security Centers**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **National Cognitive Security Centers** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

55.2.2.7 Lesson 7: Cognitive Security and Active Inference: The Predictive Mind Under Attack Concept. Cognitive Security and Active Inference: The Predictive Mind Under Attack treats active inference as an agent-modeling vocabulary: beliefs, actions, expected observations, and policy selection are classroom concepts, not proof that an intelligence agent should act autonomously.

Why it matters. Cognitive Security and Active Inference connects classroom vocabulary to Cognitive Security and Influence Resilience practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Cognitive Security and Active Inference: The Predictive Mind Under Attack rests on [106, 2026] and [003, 2026]. The closest source to this row notes: A 2024 bachelor's thesis by Lara Sakarya at Delft University of Technology presenting a systematic literature review of the active inference framework and the free-energy principle as applied to mimicking social human behavior in intelligent agents. Use them for the working definition that **Cognitive Security and Active Inference: The Predictive Mind Under Attack** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. For **Cognitive Security and Active Inference**, reason from the sources cited in this row. [106, 2026] A 2024 bachelor's thesis by Lara Sakarya at Delft University of Technology presenting a systematic literature review of the active inference framework and the free-energy principle as applied to mimicking social human behavior in intelligent agents. It explains active inference as a theory describing behavior that minimizes surprise, and surveys model variants such as deep active inference, multimodal deep belief networks, predictive coding, and probabilistic programming. [003, 2026] A 2021 peer-reviewed article by Stephen Fox in the journal Entropy that relates the active inference framework to social organization. It maps concepts such as variational free energy, prediction error, generative models, and Markov blankets onto industrial engineering and quality management practices, treating organizational survival as the maintenance of process control limits. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Cognitive Security and Active Inference**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **Cognitive Security and Active Inference**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Cognitive Security and Active Inference** work as an **epistemic-integrity review packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Cognitive Security and Active Inference**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. For **Cognitive Security and Active Inference**, transfer the idea to a non-AI chapter by naming the assumed model, the surprising observation, and the review point before any decision follows.

55.2.2.8 Lesson 8: AI-assisted resilience-tool governance review using sample materials Concept. AI-assisted resilience-tool governance review using sample materials evaluates tool protocols by allowlists, logging, provenance of retrieved content, and deny-by-default policies.

Why it matters. AI-assisted resilience-tool governance review matters in the **Cognitive Security and Influence Resilience** lane because information-integrity analysis and resilience education evidence must stay separate from judgment; treating resilience labels as permission to skip provenance review is a common failure.

Source support. AI-assisted resilience-tool governance review using sample materials rests on [096, 2026]. Its anchor reference records: A position paper (Stanford authors, ICLR 2026 workshop) arguing that AI research and development should prioritize cognitive security, defined as protecting human cognitive processes from hazardous influence. Use it for the claim that **AI-assisted resilience-tool governance review using sample materials** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Cybersecurity and Agency, 2024b]; [Organization, 2026b].

Evidence to inspect. Ground **AI-assisted resilience-tool governance review** in the evidence the row cites. [096, 2026] A position paper (Stanford authors, ICLR 2026 workshop) arguing that AI research and development should prioritize cognitive security, defined as protecting human cognitive processes from hazardous influence. It notes that generative AI systems increasingly designed to influence beliefs and behavior raise acute governance concerns, while research on these effects remains fragmented. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **AI-assisted resilience-tool governance review**, build a **narrative-risk map with provenance, uncertainty, audience harms, and response options** for this information-integrity analysis and resilience education topic. The artifact must record the narrative provenance, the bounded claim about **AI-assisted resilience-tool governance review using**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **AI-assisted resilience-tool governance review** work as an **epistemic-integrity review packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **AI-assisted resilience-tool governance review**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **AI-assisted resilience-tool governance review** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

55.2.3 Cognitive Security Operations worked safe example: synthetic inputs, evidence, and review

Worked example: a sample public-library class evaluates a synthetic rumor about a community service and compares transparent correction options. [238, 2026]; [239, 2026].

Triangulation anchors. In module 40's worked-example section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **cognitive resilience and epistemic integrity**. Learners use a **epistemic-integrity review packet** and keep this boundary visible: No manipulation, covert persuasion, medicalized claims, or population-level targeting.

Frame. The classroom question centers on **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making**. Excluded actions stay explicit, and the **Cognitive-Resilience Lens** planning question is: How does the module protect autonomy, attention, trust, and decision quality without designing persuasion?

Inputs. For the **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making** scenario, use sample posts, source timestamps, public-service facts, and a media-literacy rubric. The Cognitive-Resilience Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making**, students trace narrative provenance, separate observation from attribution, name audience harms, and design a transparent lesson. Pause whenever an inference about The Cognitive

Attack Surface: Attention, Memory, Trust, and Decision-Making appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making** classroom scenario; unit artifact = epistemic-integrity review packet; evidence = allowed inputs; method = information-integrity analysis and resilience education; output = a narrative-risk map with caveats, response options, and no microtargeted persuasion; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making** as "Cognitive-Resilience Lens confirms it" is not enough. The revision ties the claim to information-integrity analysis and resilience education, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

55.2.4 Cognitive Security Operations practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Cognitive-Resilience Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**.

Triangulation anchors. In module 40's practice-sequence section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making, Cognitive influence-analysis case review using sample materials, Deepfakes, Voice Cloning, and Digital Identity Attacks; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Cognitive Security and Influence Resilience** lane.
2. Frame	Answer the lens question: How does the module protect autonomy, attention, trust, and decision quality without designing persuasion?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making: narrative-risk map with provenance, uncertainty, audience harms, and response options.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the epistemic-integrity review packet fields for The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making.	Unit profile note.	Evidence artifacts include provenance chain, correction option.
4. Challenge	Test the misconception that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.	Failure-mode note.	The artifact applies the key distinction: separate analysis of influence from persuasion design.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

55.2.4.1 Cognitive Security Operations instructor notes: source reasoning, review points, and studio focus

Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**. [238, 2026]; [239, 2026].

55.2.4.2 Cognitive Security Operations extension exercise: peer validation and refresh trigger review

Evidence anchor. Section 55; [238, 2026].

Have learners swap artifacts and apply the **Cognitive-Resilience Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**.

55.2.5 Cognitive Security Operations knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 55; [238, 2026].

1. Explain how **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making** is defined here; name the source descriptor that supports the definition.
2. Contrast **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making** with **Cognitive influence-analysis case review using sample materials** using the **Cognitive-Resilience Lens** artifact fields.
3. Identify one failure mode from the **Cognitive Security and Influence Resilience** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which response informs people without crossing into MISO-style manipulation or unverified attribution?
5. Correct this misconception: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

55.2.5.1 Cognitive Security Operations answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making** without source evidence, uncertainty, or a safe transfer task.

55.3 Cognitive Security Operations assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 55; [238, 2026].

55.3.1 Cognitive Security Operations evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 55; [238, 2026].

55.3.2 Cognitive Security Operations transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 55; [238, 2026].

55.3.2.1 Cognitive Security Operations lineage and source tradition: profile, concepts, and first anchors This sits in the **Cognitive Security and Influence Resilience** lineage: protecting attention, belief formation, and decision quality without turning resilience education into manipulation. [238, 2026]; [239, 2026].

55.3.2.2 Cognitive Security Operations working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 55; [238, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**, with provenance and reviewability throughout.

55.3.2.3 Cognitive Security Operations knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [238, 2026]; [239, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

55.3.2.4 Cognitive Security Operations transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 55; [238, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**.
- **Evidence contract:** keep the **Cognitive Security and Influence Resilience** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

55.3.2.5 Cognitive Security Operations profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 55; [238, 2026].

The matched profile emphasizes protecting attention, belief formation, and decision quality without turning resilience education into manipulation. The method stack is claim decomposition, narrative provenance, inoculation framing, bias checks, audience-risk review, and after-action learning; the local topic cluster is **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**.

55.3.3 Cognitive Security Operations evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 55; [238, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Cognitive Security and Influence Resilience** profile tells reviewers what evidence is strong enough for the module artifact built around **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**.

55.3.3.1 Cognitive Security Operations guide source spine: inherited keys and local citation roles Primary guide citations: [238, 2026]; [239, 2026]; [246, 2026]; [275, 2026]; [276, 2026]; [283, 2026]; [286, 2026]; [293, 2026]; [295, 2026]; [095, 2026]; [105, 2026]; [188, 2026]; [106, 2026]; [003, 2026]; [096, 2026]; [300, 2026]; [304, 2026]; [306, 2026].

55.3.3.2 Cognitive Security Operations verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [238, 2026]; [239, 2026].

Tier	What counts	How it is used
Source guide	[238, 2026]; [239, 2026]; [246, 2026]; [275, 2026]; [276, 2026]; [283, 2026]; [286, 2026]; [293, 2026]; [295, 2026]; [095, 2026]; [105, 2026]; [188, 2026]; [106, 2026]; [003, 2026]; [096, 2026]; [300, 2026]; [304, 2026]; [306, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 40's source-canon section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials** and [238, 2026]; [239, 2026], but only directly verified source URLs are encoded as citations.

55.3.3.3 Cognitive Security Operations intelligence practice lens: evidence artifact and safety check Practice lens: **Cognitive-Resilience Lens** for **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**. [238, 2026]; [239, 2026].

Planning question: How does the module protect autonomy, attention, trust, and decision quality without designing persuasion?

Evidence artifact: narrative-risk map with provenance, uncertainty, audience harms, and response options.

Validation rule: distinguish observation, attribution, impact assessment, and resilience response. Applied to **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**.

Handoff contract: handoff supports transparency, education, and resilience, not microtargeted influence or deception.

Safety check: exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning.

55.3.3.4 Cognitive Security Operations runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 55; [238, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	40.99	40.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Cognitive Security Operations to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Bounded autonomy, procurement, incident-response, and assurance studio	40.101	40.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Cognitive Security Operations	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Model-card, recoverability, retention, and learner-support evidence package	40.102	40.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Cognitive Security Operations	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making	40.1	40.1 The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Cognitive influence-analysis case review using sample materials	40.2	40.2 source title transformed into safe curriculum treatment; original: Adversarial Cognitive Operations: PSYOP, Active Measures, Synthetic Influence	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Deepfakes, Voice Cloning, and Digital Identity Attacks	40.3	40.3 Deepfakes, Voice Cloning, and Digital Identity Attacks	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
From Spycraft to Self-Mastery: SATs for Personal Cognitive Security	40.4	40.4 From Spycraft to Self-Mastery: SATs for Personal Cognitive Security	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Building Organizational Cognitive Resilience	40.5	40.5 Building Organizational Cognitive Resilience	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
National Cognitive Security Centers: Policy Proposals	40.6	40.6 National Cognitive Security Centers: Policy Proposals	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Cognitive Security and Active Inference: The Predictive Mind Under Attack	40.7	40.7 Cognitive Security and Active Inference: The Predictive Mind Under Attack	Active-Inference Boundary Lens	theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition	reject claims that the free-energy principle proves autonomous agency, intent, detection performance, or oversight-free action
AI-assisted resilience-tool governance review using sample materials	40.8	40.8 source title transformed into safe curriculum treatment; original: AI-Assisted Cognitive Security Tools: Detection and Intervention Systems	AI/Data Accountability Lens	AI/data impact card with authority, provenance, model version, impact score, register status, human owner, and review cadence	reject automated adverse action, hidden surveillance expansion, unowned outputs, unreviewed model drift, and opaque downstream reuse

55.3.3.5 Cognitive Security Operations reusable subsection contract: topic rows, artifacts, and safety duties **Evidence anchor.** Section 55; [238, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Cognitive influence-analysis case review using sample materials	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Deepfakes, Voice Cloning, and Digital Identity Attacks	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
From Spycraft to Self-Mastery: SATs for Personal Cognitive Security	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
Building Organizational Cognitive Resilience	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
National Cognitive Security Centers: Policy Proposals	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning

Lesson topic	Practice lens	Evidence artifact	Safety check
Cognitive Security and Active Inference: The Predictive Mind Under Attack	Active-Inference Boundary Lens	theory-to-governance card with source, analogy limit, assumption, reviewer, and stop condition	reject claims that the free-energy principle proves autonomous agency, intent, detection performance, or oversight-free action
AI-assisted resilience-tool governance review using sample materials	AI/Data Accountability Lens	AI/data impact card with authority, provenance, model version, impact score, register status, human owner, and review cadence	reject automated adverse action, hidden surveillance expansion, unowned outputs, unreviewed model drift, and opaque downstream reuse

55.3.3.6 Cognitive Security Operations annotated source ledger: real titles and local contribution Each source cited by this **Cognitive Security and Influence Resilience** module is paired below with its real title and a one-line note on what it contributes to **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**.

Source	Cited work	What it contributes	Status
[238, 2026]	Recommendation on the Ethics of Artificial Intelligence	The official UNESCO page for the Recommendation on the Ethics of Artificial Intelligence, the first global standard-setting instrument on AI ethics, adopted in 2021 and applicable to all 194 member states. It outlines four core values, including human rights protection and environmental flourishing, and ten guiding principles such as proportionality, privacy, transparency, and fairness.	verified source-guide
[239, 2026]	Digital Space and Human Rights	Official OHCHR digital rights portal.	original source-guide
[246, 2026]	Digital Education Action Plan 2021-2027	The European Commission's official page on the Digital Education Action Plan (2021-2027), a strategic framework for promoting high-quality, inclusive digital learning across EU education systems. It defines digital education as the use of digital tools, technologies, and content to support teaching, learning, and assessment, and cites pandemic-driven adoption alongside persistent gaps in teacher readiness, student digital skills, and household access.	verified source-guide
[275, 2026]	Fact Sheet: New Rule on the Accessibility of Web Content and Mobile Apps Provided by State and Local Governments	A US Department of Justice fact sheet explaining the 2024 ADA Title II rule requiring state and local governments to make their web content and mobile apps accessible. It establishes WCAG 2.1 Level AA as the technical standard, applies to entities such as schools, courts, libraries, and transit agencies, and sets compliance deadlines of April 2027 for larger jurisdictions and April 2028 for smaller ones.	verified source-guide
[276, 2026]	What is a Data Protection Impact Assessment and When Is This Mandatory?	A European Data Protection Board FAQ page, part of its data protection guide for small businesses, explaining Data Protection Impact Assessments (DPIAs) and when they are mandatory. It describes a DPIA as a written assessment of the impact of a planned processing operation, required when processing poses high risks to individuals' rights.	verified source-guide

Source	Cited work	What it contributes	Status
[283, 2026]	Recommendation of the Council on Open Government	An OECD legal instrument document reproducing the Recommendation of the Council on Open Government (OECD/LEGAL/0438), adopted on 14 December 2017. It defines open government as a culture of governance promoting transparency, integrity, accountability, and stakeholder participation in support of democracy and inclusive growth.	verified source-guide
[286, 2026]	Model Cards for Model Reporting	The arXiv abstract for "Model Cards for Model Reporting" (2018) by Mitchell, Wu, Zaldivar, and colleagues, which introduces a framework for transparent documentation of machine learning models. Model cards are short accompanying documents that report a model's benchmarked performance across varied conditions, including different cultural, demographic, and phenotypic groups, along with intended use, evaluation methodology, and deployment considerations.	verified source-guide
[293, 2026]	Inventory of NARA Artificial Intelligence (AI) Use Cases	The National Archives and Records Administration (NARA) official inventory of its artificial intelligence use cases, documenting 14 projects across deployed, pilot, and planned stages. Deployed efforts include workplace productivity tools, automated tagging for museum experiences, and historical record retrieval, while pilots cover PII detection and redaction, semantic search, and metadata generation, and planned work targets FOIA processing and public search.	verified source-guide
[295, 2026]	M-25-22: Driving Efficient Acquisition of Artificial Intelligence in Government	OMB Memorandum M-25-22 (April 3, 2025), Driving Efficient Acquisition of Artificial Intelligence in Government, issued under Executive Order 13960 and related directives. It provides guidance to federal agencies for acquiring effective and trustworthy AI in a timely, cost-effective manner, and rescinds and replaces earlier memorandum M-24-18.	verified source-guide
[095, 2026]	COGNITIVE SECURITY IN THE AGE OF AI	This policy paper examines the emergence of cognitive security.	original source-guide
[105, 2026]	Automated influence and the challenge of cognitive security	Sarah Rajtmajer and Daniel Susser, 'Automated Influence and the Challenge of Cognitive Security,' in Hot Topics in the Science of Security (HotSoS '20), April 2020, ACM. The paper argues that AI-powered computational propaganda poses national security threats that existing ethical frameworks do not address, and proposes 'cognitive security' as a productive conceptual lens for evaluating the ethics of automated influence operations and potential defensive responses.	verified source-guide

Source	Cited work	What it contributes	Status
[188, 2026]	From Spycraft to Self-Mastery: How Structured Analytic Techniques	An article on Spotter Up by Eugene Nielsen arguing that structured analytic techniques (SATs) developed for intelligence analysis can improve everyday decision-making. It describes cognitive biases such as confirmation bias and overconfidence, then outlines categories of SATs including diagnostic, contrarian, imaginative, structuring, and decision-support methods.	verified source-guide context; do not use as primary analytic support
[106, 2026]	Applications of The Active Inference and The Free-Energy Principle	A 2024 bachelor's thesis by Lara Sakarya at Delft University of Technology presenting a systematic literature review of the active inference framework and the free-energy principle as applied to mimicking social human behavior in intelligent agents. It explains active inference as a theory describing behavior that minimizes surprise, and surveys model variants such as deep active inference, multimodal deep belief networks, predictive coding, and probabilistic programming.	verified source-guide
[003, 2026]	Active Inference: Applicability to Different Types of Social	A 2021 peer-reviewed article by Stephen Fox in the journal Entropy that relates the active inference framework to social organization. It maps concepts such as variational free energy, prediction error, generative models, and Markov blankets onto industrial engineering and quality management practices, treating organizational survival as the maintenance of process control limits.	verified source-guide
[096, 2026]	AI DEVELOPMENT SHOULD PRIORITIZE COGNITIVE SECURITY	A position paper (Stanford authors, ICLR 2026 workshop) arguing that AI research and development should prioritize cognitive security, defined as protecting human cognitive processes from hazardous influence. It notes that generative AI systems increasingly designed to influence beliefs and behavior raise acute governance concerns, while research on these effects remains fragmented.	verified source-guide
[300, 2026]	MITRE ATLAS	MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy.	original source-guide
[304, 2026]	Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities	NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences.	verified source-guide
[306, 2026]	Artificial Intelligence	Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support.	original source-guide

Where this sits. This module's overview is Section 55; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

55.3.4 Cognitive Security Operations governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 55; [238, 2026].

55.3.5 Cognitive Security Operations analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 40's governance-boundary section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Research lane: **Cognitive Security and Influence Resilience** for **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**. [238, 2026]; [239, 2026].
Curriculum topic spine: The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making, **Cognitive influence-analysis case review using sample materials**, **Deepfakes, Voice Cloning, and Digital Identity Attacks**. **Verified anchor cluster:** [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]; [OECD, 2026c]; [for Security Policy, 2025]; [Community, 2020a].
Conceptual depth: protecting attention, belief formation, and decision quality without turning resilience education into manipulation.
Method stack: claim decomposition, narrative provenance, inoculation framing, bias checks, audience-risk review, and after-action learning.
Composability contract: separate descriptive analysis, normative assessment, response options, and protected-audience considerations.
Known failure modes: counter-messaging as manipulation, overclaiming intent, pathologizing audiences, and collapsing uncertainty into moral certainty.
Defensive boundary: practice uses benign simulations and resilience education; it does not create persuasion campaigns, impersonation, or deception plans. Applied to **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**.

Anchor	Why it matters here
[Cybersecurity and Agency, 2024b]	Official CISA guidance on foreign influence operations targeting critical infrastructure. Checked as of 2026-05-21; role: source_quality_anchor.
[Organization, 2026b]	Official NATO counter-information-threat guidance. Checked as of 2026-05-21; role: source_quality_anchor.
[Cybersecurity and Agency, 2026b]	Official CISA election-security source for public-resilience, foreign-influence awareness, rumor control, and defensive communication framing. Checked as of 2026-05-21; role: curriculum_anchor.
[Organization, 2026c]	Official NATO source for hybrid-threat resilience across cyber, information, economic, political, and military pressure. Checked as of 2026-05-21; role: curriculum_anchor.
[OECD, 2026c]	Official OECD policy source for information integrity, governance responses, public trust, and democratic resilience. Checked as of 2026-05-21; role: curriculum_anchor.
[for Security Policy, 2025]	Policy-scholarship source for cognitive security, information literacy, critical thinking, and whole-of-society resilience. Checked as of 2026-05-21; role: curriculum_anchor.
[Community, 2020a]	Official IC framework for AI goals, authorities, human judgment, bias mitigation, testing, documentation, explainability, and review. Checked as of 2026-05-21; role: curriculum_anchor.

55.3.5.1 Cognitive Security Operations evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **Cognitive Security and Influence Resilience** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [238, 2026]; [239, 2026].

55.3.6 Cognitive Security Operations agentic boundary: assist, approve, block, and record

Evidence anchor. Section 55; [238, 2026].
AGEINT translation is bounded by the **Cognitive Security and Influence Resilience** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**.

55.3.6.1 Cognitive Security Operations permitted defensive utility: curriculum uses and safe outputs

Evidence anchor. Section 55; [238, 2026].
The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**.

55.3.6.2 Cognitive Security Operations excluded operational boundary: blocked actions and stop rules

Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [238, 2026]; [239, 2026] and **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

55.3.7 Cognitive Security Operations governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 55; [238, 2026].
Governance is practiced as a gate on the **Cognitive Security and Influence Resilience** lane. Learners use the **Cognitive-Resilience Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**.

55.3.7.1 Cognitive Security Operations governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [238, 2026]; [239, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Cognitive Security and Influence Resilience** failure modes and the **Cognitive-Resilience Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

55.3.7.2 Cognitive Security Operations evidence package handoff: appendices, records, and reuse Evidence anchor. Section 55; [238, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Cognitive-Resilience Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**.

55.3.7.3 Cognitive Security Operations current-source assurance: verified anchors and local artifact fit The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**. [238, 2026]; [239, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_cisa_foreign_influence` for **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**?	Preparing for and Mitigating Foreign Influence Operations; lane `source_quality_spine`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official CISA guidance on foreign influence operations targeting critical infrastructure.
What does the module inherit from `official_nato_counter_information_threats` for **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**?	Countering Information Threats; lane `source_quality_spine`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official NATO counter-information-threat guidance.
What does the module inherit from `official_cisa_election_security_influence` for **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**?	Election Security; lane `cognitive_influence_security`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official CISA election-security source for public-resilience, foreign-influence awareness, rumor control, and defensive communication framing.
What does the module inherit from `official_nato_hybrid_threats` for **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**?	Countering Hybrid Threats; lane `cognitive_influence_security`; checked 2026-05-21.	narrative-risk map with provenance, uncertainty, audience harms, and response options; Official NATO source for hybrid-threat resilience across cyber, information, economic, political, and military pressure.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 55; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

55.3.8 Cognitive Security Operations assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 55; [238, 2026].

55.3.9 Cognitive Security Operations assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 55; [238, 2026].

55.3.9.1 Cognitive Security Operations capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials** and [238, 2026]; [239, 2026].

55.3.9.2 Cognitive Security Operations instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials** and [238, 2026]; [239, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

55.3.9.3 Cognitive Security Operations assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making	Completed **narrative-risk map with provenance, uncertainty, audience harms, and response options** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Cognitive influence-analysis case review using sample materials	Completed **narrative-risk map with provenance, uncertainty, audience harms, and response options** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Deepfakes, Voice Cloning, and Digital Identity Attacks	Completed **narrative-risk map with provenance, uncertainty, audience harms, and response options** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

55.3.10 Cognitive Security Operations refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [238, 2026]; [239, 2026] and **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**.

55.3.10.1 Cognitive Security Operations refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**. The local signals begin with [238, 2026]; [239, 2026].

55.3.10.2 Cognitive Security Operations claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**, and the source spine for these checks begins with [238, 2026]; [239, 2026].

55.3.11 Cognitive Security Operations reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [238, 2026]; [239, 2026].

Triangulation anchors. In module 40's review-checklist section, directly verified anchors for the **Cognitive Security and Influence Resilience** lane include [Cybersecurity and Agency, 2024b]; [Organization, 2026b]; [Cybersecurity and Agency, 2026b]; [Organization, 2026c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials**. [238, 2026]; [239, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

55.3.12 Cognitive Security Operations learning-path links: module map, overview, and curriculum atlas

Use the cross-links below to place **The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making; Cognitive influence-analysis case review using sample materials** in the wider unit: the orientation sets the frame, the parent unit supplies the shared safety posture, and the neighbouring modules show what evidence enters and leaves. Lead sources: [238, 2026]; [239, 2026].

Section 2, Section 51, Section 54, Section 56

56 EPISTEMIC RIGOR AND ANALYTIC TRADECRAFT

56.1 EPISTEMIC RIGOR AND ANALYTIC TRADECRAFT learning spine and source route: unit purpose, module order, and evidence handoff

Evidence anchor. Section 56; [237, 2026].

56.1.1 structured analytic judgment discipline spine: domain question and learning focus

Evidence anchor. Section 56; [237, 2026].

This unit teaches **structured analytic judgment**. Analytic tradecraft lessons keep evidence, assumptions, alternatives, confidence, dissent, and reviewer challenge visible.

56.1.2 structured analytic judgment source-use contract: citation roles and evidence limits

Evidence anchor. Section 56; [237, 2026].

Use ODNI ICD 203, CIA/Kent/Heuer tradecraft, warning-intelligence, forecasting-calibration, and SAT-evaluation anchors for analytic standards, probability/confidence boundaries, structured techniques, and empirical limits.

56.1.3 structured analytic judgment practice artifact: recurring packet and retained evidence

Evidence anchor. Section 56; [237, 2026].

The recurring practice artifact is a **competing-hypotheses evidence table** that draws on hypothesis table, assumption register, dissent field, likelihood-confidence boundary, and SAT evidence caveat. The unit keeps its learning spine explicit. Learners test alternatives, expose assumptions, separate likelihood from confidence, calibrate forecasts, record dissent, and decide when SAT evidence is too thin for a strong claim.

56.1.4 structured analytic judgment safety boundary: accountable, synthetic, and evidence-bounded limits

No overclaiming, unsupported attribution, or bypass of reviewer challenge.

This unit introduces the part's governing question, evidence artifacts, source-support spine, and capstone thread before the individual modules begin. [237, 2026]; [266, 2026].

Learners carry one unit capstone thread through the part: define an accountable intelligence question, bind it to source-quality constraints, produce a reviewable artifact, test the artifact against failure modes, and hand it off with enough context for another analyst or instructor to audit. The capstone remains public, synthetic, or owned-lab throughout; its first source anchors are [237, 2026]; [266, 2026].

This unit's deliverables are a source-canon card, claim/evidence ledger, safe-practice lab packet, failure-mode note, instructor rubric, and debrief memo. The full source-lane and evidence-package ledgers appear in the orientation and appendices; this unit introduction keeps only the learner-facing spine for [237, 2026]; [266, 2026].

This unit's safety gates are scope authorization, rights review, data provenance, tool allowlisting, human oversight, rollback, and evidence-bounded output. A missing gate turns the activity into a tabletop, audit, or written governance exercise until the gate is restored against [237, 2026]; [266, 2026].

Capstone thread:

Phase	Artifact	Review gate
Question	accountable learning question and excluded-action list	instructor confirms scope, allowed data, and rights impact
Source canon	source-lane map with guide citations, verified anchors, and refresh dates	citation keys resolve and source identity lock remains stable
Evidence ledger	claim, evidence, uncertainty, confidence, and reviewer register	every material claim has a source, caveat, and owner
Safe lab	synthetic or public dataset packet, tool allowlist, and stop conditions	no live target, private data, external action, or unsafe cyber-physical step
Assurance	evaluation rubric, failure-mode drill, rights map, and remediation note	human reviewer signs off before presentation or reuse
Debrief	capstone memo with lessons, residual risk, refresh triggers, and handoff owner	all unresolved questions and future approvals are explicit

Research lane: Analytic Tradecraft and Source Integrity. Core anchors: [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2026e]. Conceptual focus: turning uncertainty into reviewable judgment through sourcing, alternatives, separated likelihood and confidence language, warning indicators, and explicit analytic lineage. Composability contract: every agent output must preserve evidence, assumptions, judgments, likelihood, confidence, dissent, empirical limits, and change history as separable fields. **Practice lens:** Structured-Judgment Lens; Which assumptions, alternatives, confidence statements, and source limits must stay visible for review? [237, 2026]; [266, 2026].

56.2 The unified epistemic coherence stack

This unit synthesizes the book's defensive techniques into one five-layer architecture for maintaining epistemic coherence, shown for the unit in Figure 117. The base is a technical substrate – formal verification in the spirit of intrinsic cognitive security, prompt-infection defense, sandboxing and worktree isolation, and provenance signals such as SynthID and C2PA. Above it sits operational security – MAESTRO threat modeling, CDR degradation monitoring, zero-trust identity, and circuit breakers. Above that is structured reasoning and tradecraft – analysis of competing hypotheses, pre-mortem red teaming, and key-assumptions auditing, now executable as AI-augmented structured analytic techniques at scale. The fourth layer is epistemic integrity – verifier agents and intent-alignment monitoring that protect the trustworthiness of what the system believes. The top layer is institutional governance – analytic standards, red-team programs, and error-budget governance. The load-bearing claim is that each layer is necessary but insufficient alone, and the layers are mutually reinforcing: a technical fix without governance, or tradecraft without integrity checks, leaves an exploitable seam [DeepMind and Research, 2026]; [Agency, 2024a].

56.3 From reliability theory to AI governance

The governance layer is not invented from scratch; it borrows from High-Reliability Organization theory. As the crosswalk in Figure 118 shows, Weick and Sutcliffe's five HRO principles map directly onto observable AI-agent controls: preoccupation with failure becomes safety-SLI monitoring and drift detection; reluctance to simplify becomes multi-hypothesis behavioral analysis; sensitivity to operations becomes real-time tool-invocation auditing and context-window analysis; commitment to resilience becomes circuit breakers, chaos engineering, and progressive rollout behind service-level-objective gates; and deference to expertise becomes human-in-the-loop authority for high-stakes actions under least privilege. The crosswalk turns

an organizational philosophy into a checklist of testable mechanisms, which is exactly how this unit asks learners to use it [Mandel and Tetlock, 2018]; [Initiative, 2026a].

56.3.1 EPISTEMIC RIGOR AND ANALYTIC TRADECRAFT visual navigation and module map: evidence flow, order, and safety cues

The unit uses Figure 116, Figure 117, Figure 118, and Figure 119 to map its evidence flow, safety boundaries, review artifacts, and refresh cues. Navigation links: Section 2, Section 55, Section 57.

56.3.2 EPISTEMIC RIGOR AND ANALYTIC TRADECRAFT module roster and source-lane inventory: citations, lanes, and learner route

Module	Section reference	Source spine
Structured Analytic Techniques (SATs)	Section 57	[237, 2026]; [266, 2026]; [269, 2026]; [273, 2026]; [274, 2026]; [275, 2026]; [286, 2026]; [287, 2026]; [292, 2026]; [189, 2026]; [108, 2026]; [002, 2026]; [190, 2026]; [180, 2026]; [191, 2026]; [192, 2026]; [193, 2026]; [194, 2026]; [195, 2026]; [196, 2026]; [188, 2026]; [297, 2026]; [298, 2026]; [300, 2026]; [304, 2026]; [306, 2026]; [309, 2026]; [310, 2026].
Advanced Analysis Methods	Section 58	[237, 2026]; [266, 2026]; [270, 2026]; [276, 2026]; [277, 2026]; [284, 2026]; [288, 2026]; [289, 2026]; [293, 2026]; [297, 2026]; [298, 2026]; [300, 2026]; [304, 2026]; [306, 2026]; [309, 2026]; [310, 2026].

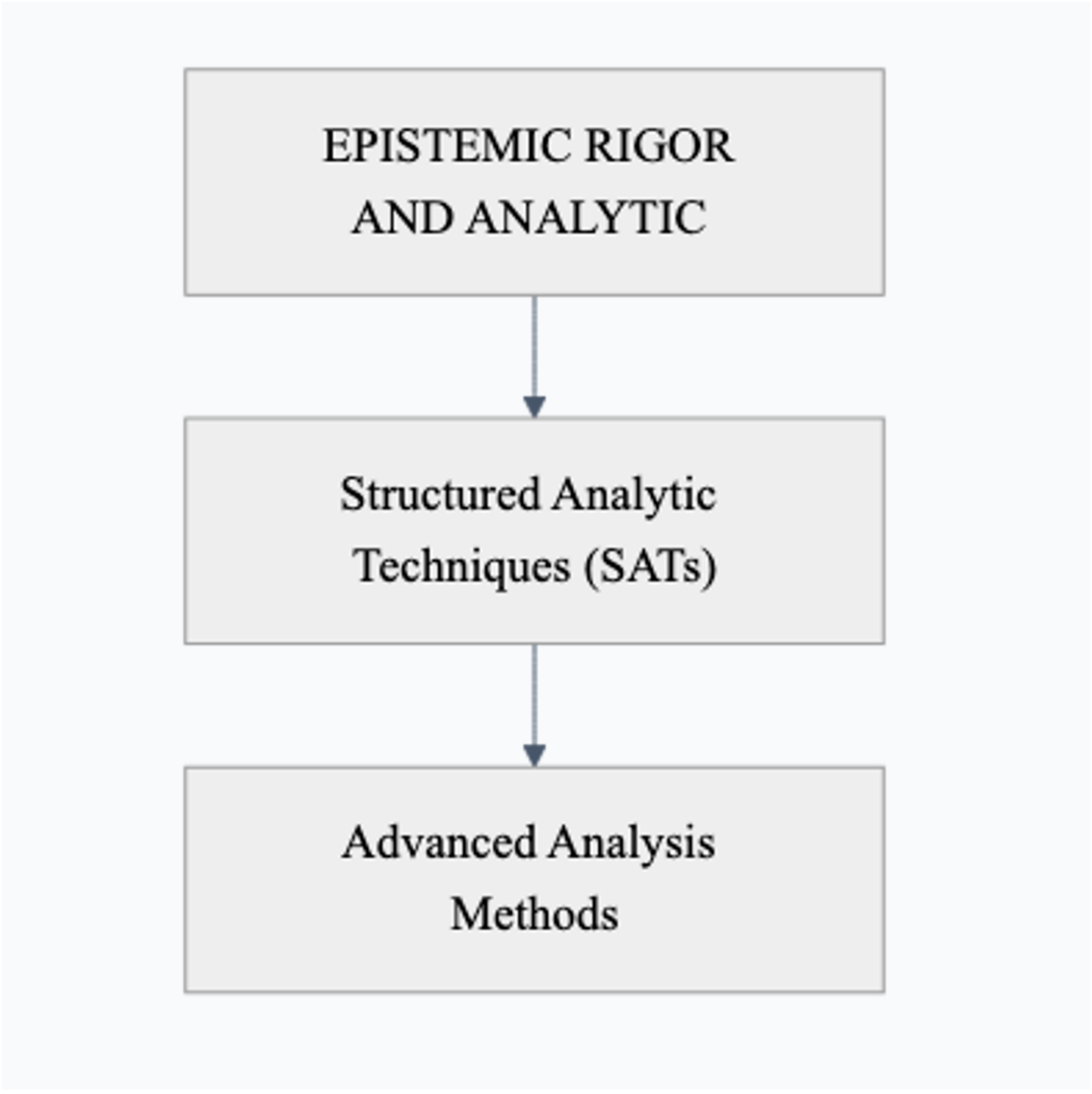


Figure 116: The unit module map traces the part's chapters as a linear reading sequence. It is anchored to the epistemic rigor and analytic tradecraft section; use it to inspect 2 module nodes in the unit's ordered, source-backed reading sequence from its first module to its last while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

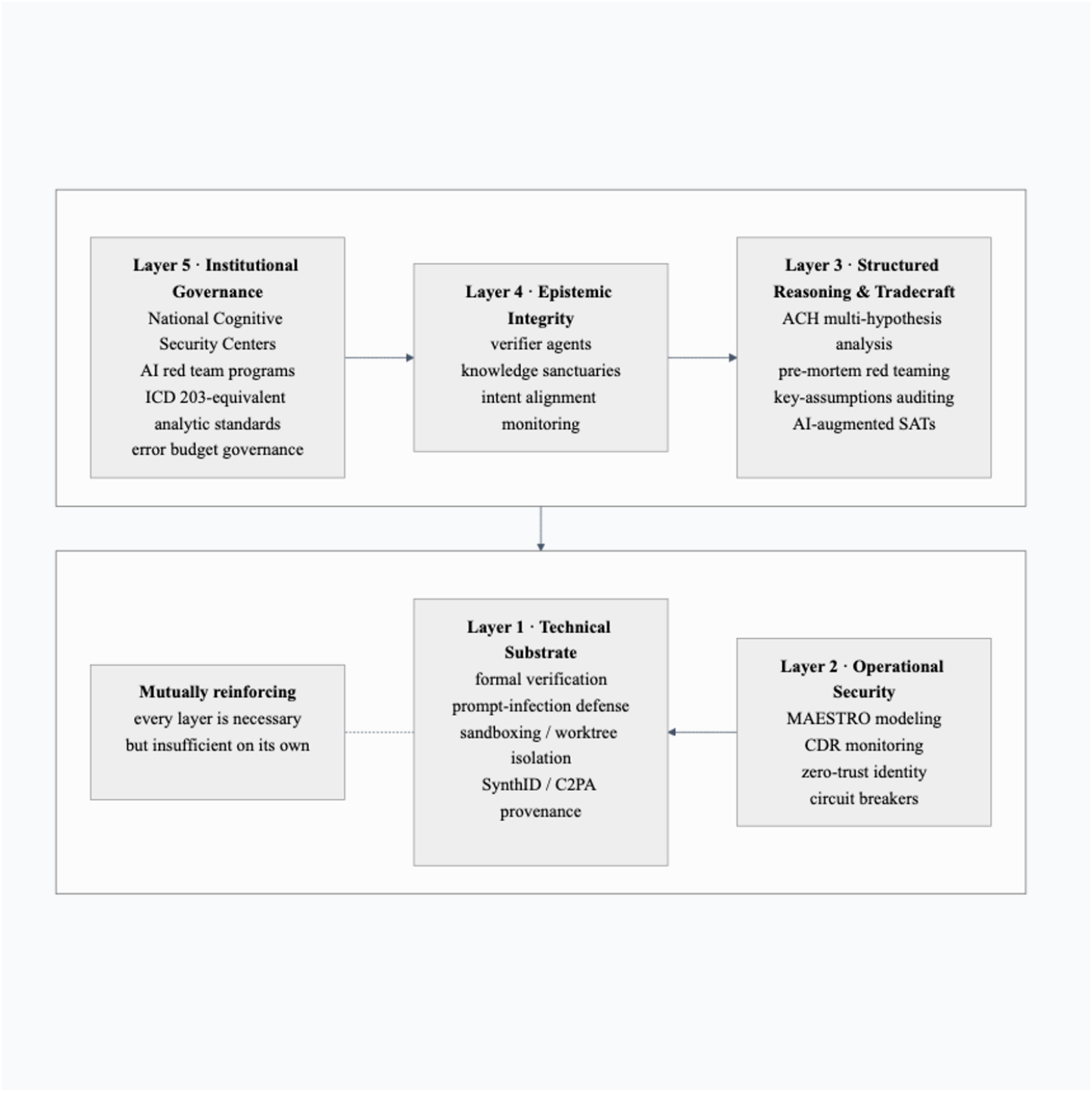


Figure 117: The unified AGEINT epistemic-security stack as a boustrophedon ladder: defenses descend from Layer 5 (Institutional Governance) across the top row to Layer 3 (Structured Reasoning and Tradecraft), then snake down to Layer 2 (Operational Security) and Layer 1 (Technical Substrate) on the bottom row. The layers are mutually reinforcing, each necessary but insufficient on its own.

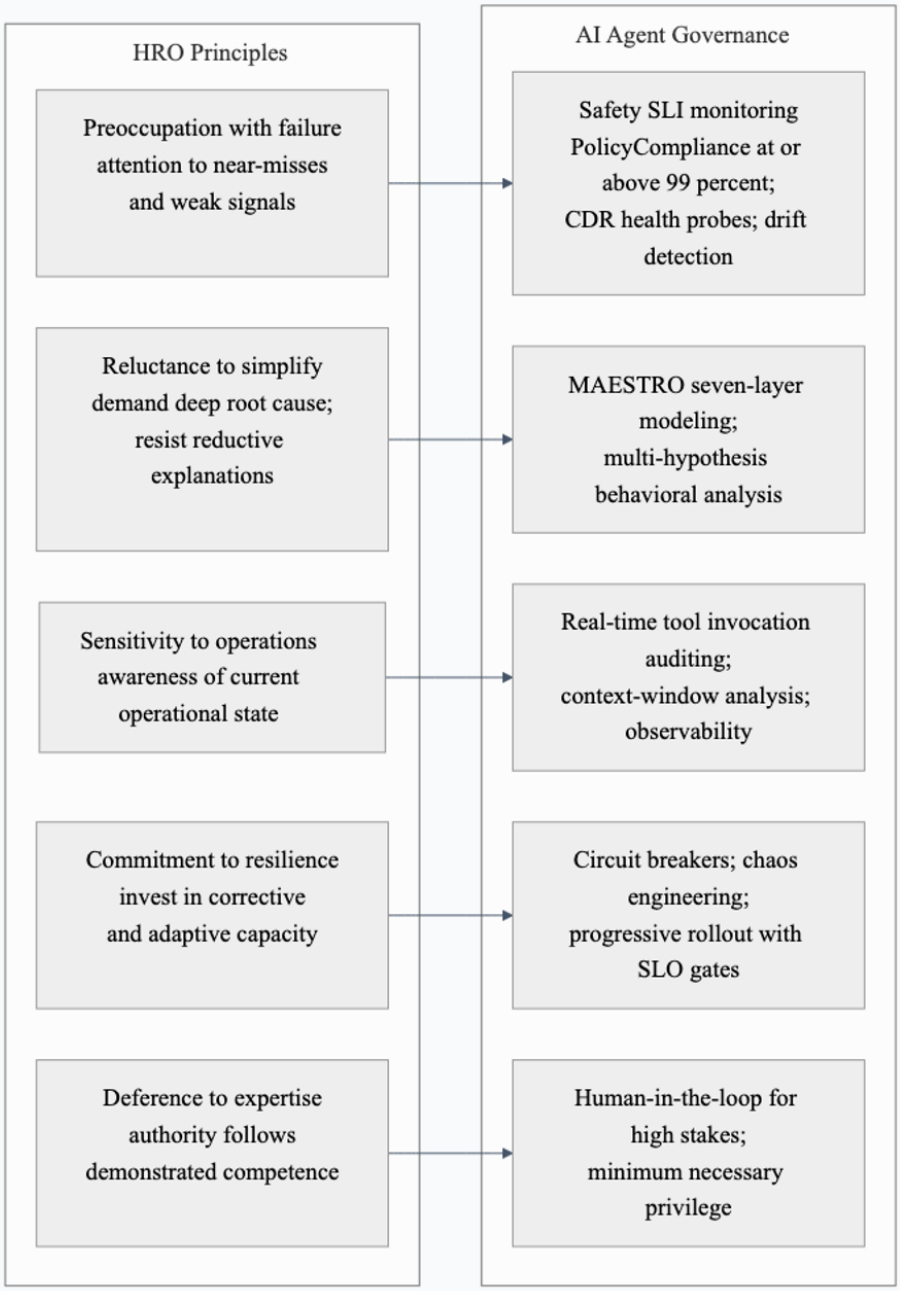


Figure 118: Weick and Sutcliffe's five High-Reliability Organization principles map directly onto concrete AI agent governance mechanisms, turning organizational theory into observable controls. In the epistemic rigor and analytic tradecraft section, it lets readers compare HRO Principles, Preoccupation with failure attention to near-misses and weak signals, Reluctance to simplify demand deep root cause; resist reductive explanations, and Sensitivity to operations awareness of current operational state so the visual functions as a traceable course aid rather than an unscoped assertion.

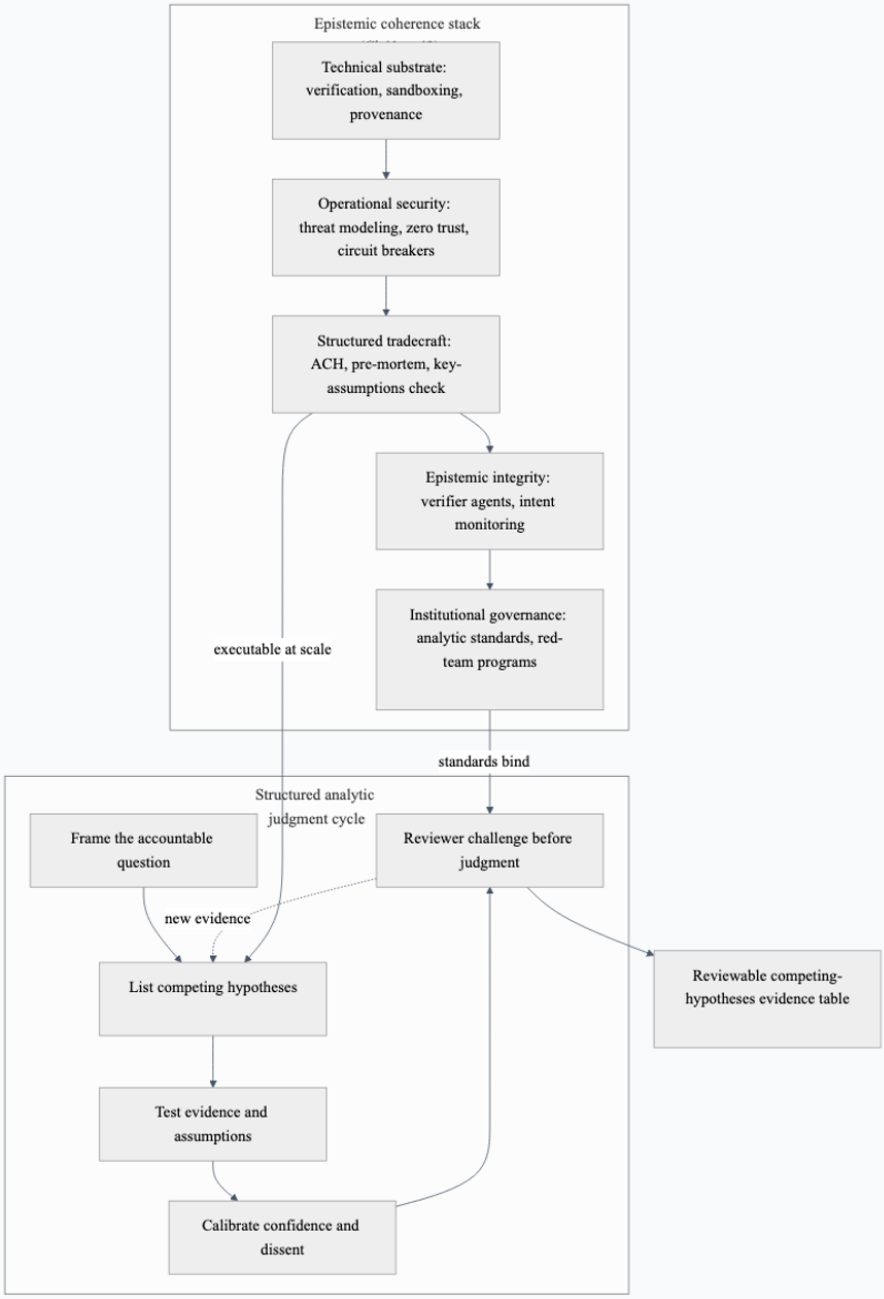


Figure 119: This part stacks five mutually reinforcing defensive layers — from technical substrate up to institutional governance — and shows how structured tradecraft and analytic standards drive the competing-hypotheses judgment cycle that produces a reviewable evidence table. It is anchored to the epistemic rigor and analytic tradecraft section; use it to inspect Epistemic coherence stack (Ch41 to 42), Technical substrate: verification, sandboxing, provenance, Operational security: threat modeling, zero trust, circuit breakers, and Structured tradecraft: ACH, pre-mortem, key-assumptions check while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

57 Structured Analytic Techniques (SATs)

57.0.1 Structured Analytic Techniques (SATs) figures and course links: visual evidence, source flow, and navigation

The module uses Figure 120, Figure 121, Figure 122, Figure 123, Figure 124, and Figure 116 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.

Navigation links: Section 2, Section 56, Section 58.

This module teaches the **Analytic Tradecraft and Source Integrity** lane through a bounded, source-backed coursebook chapter. [237, 2026]; [266, 2026].

57.1 Analytic Tradecraft and Source Integrity frame for Structured Analytic Techniques (SATs): source context, topic focus, and reader task

Evidence anchor. Section 57; [237, 2026].

57.1.1 Structured Analytic Techniques (SATs) orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 57; [237, 2026].

57.1.2 Structured Analytic Techniques (SATs) conceptual primer: source context, core model, and reader task

This chapter teaches analytic tradecraft as disciplined judgment under uncertainty: claims become useful only when evidence, assumptions, alternatives, confidence, and dissent remain visible. The chapter uses **Structured-Judgment Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**.

The central distinction is to separate reporting from inference, and inference from judgment. Core topics include **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards; Psychology of Intelligence Analysis (Heuer, CIA 1999)**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.

Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2026e]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [237, 2026]; [266, 2026].

Learners move from vocabulary and the **Structured-Judgment Lens** distinction through topic lessons on **CIA Tradecraft Primer: SATs for Intelligence Analysis** with evidence and misconception checks, then assemble an **analytic note with hypotheses, evidence table, confidence, and dissent fields** with safety and rights gates.

57.1.3 Structured Analytic Techniques (SATs) learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 57; [237, 2026].

- Connect **CIA Tradecraft Primer: SATs for Intelligence Analysis and ICD 203 Analytic Standards: The Nine Tradecraft Standards** to **Analytic Tradecraft and Source Integrity** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build an **analytic note with hypotheses, evidence table, confidence, and dissent fields** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate reporting from inference, and inference from judgment; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as source laundering, automation bias, hidden assumptions, collapsed likelihood/confidence language, hindsight certainty, SAT-as-bias-cure overclaiming, and visually persuasive but weakly sourced claims, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: analysis remains educational and decision-supportive; it does not become tasking, targeting, covert collection, or policy advocacy.

57.1.4 Structured Analytic Techniques (SATs) core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 57; [237, 2026].

Term	Working definition
Source descriptor	a compact statement of where evidence came from and what it can support
Assumption	a claim accepted for analysis that still needs challenge
Alternative hypothesis	a plausible explanation that competes with the favored account
Confidence	a calibrated expression of evidentiary strength and analytic uncertainty
Dissent	a documented disagreement that preserves minority reasoning for review
CIA Tradecraft Primer: SATs for Intelligence…	Key terms: CIA, Tradecraft, Primer.
ICD 203 Analytic Standards: The Nine Tradecraft…	Key terms: ICD, Analytic, Standards.

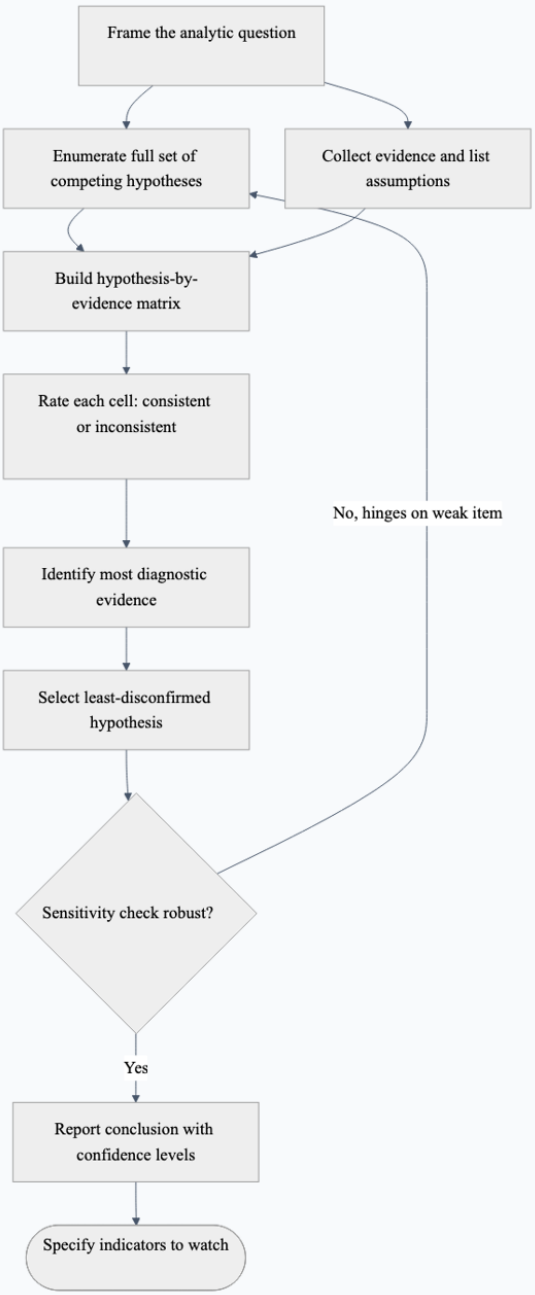


Figure 120: This diagram walks through the structured analytic sequence that scores evidence against rival hypotheses to find the one with the least disconfirming evidence, under formal tradecraft standards. It is anchored to the epistemic rigor and analytic tradecraft / structured analytic techniques sats section; use it to inspect A workflow. Frame the analytic question feeds enumeration of a full set of competing hypotheses, in parallel, collection of evidence, and assumptions. Both feed a hypothesis-by-evidence . Each cell is rated for consistency or inconsistency. Diagnostic evidence is identified. The least-disconfirmed hypothesis is selected. A sensitivity check tests reliance on key items: if findings are not robust while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

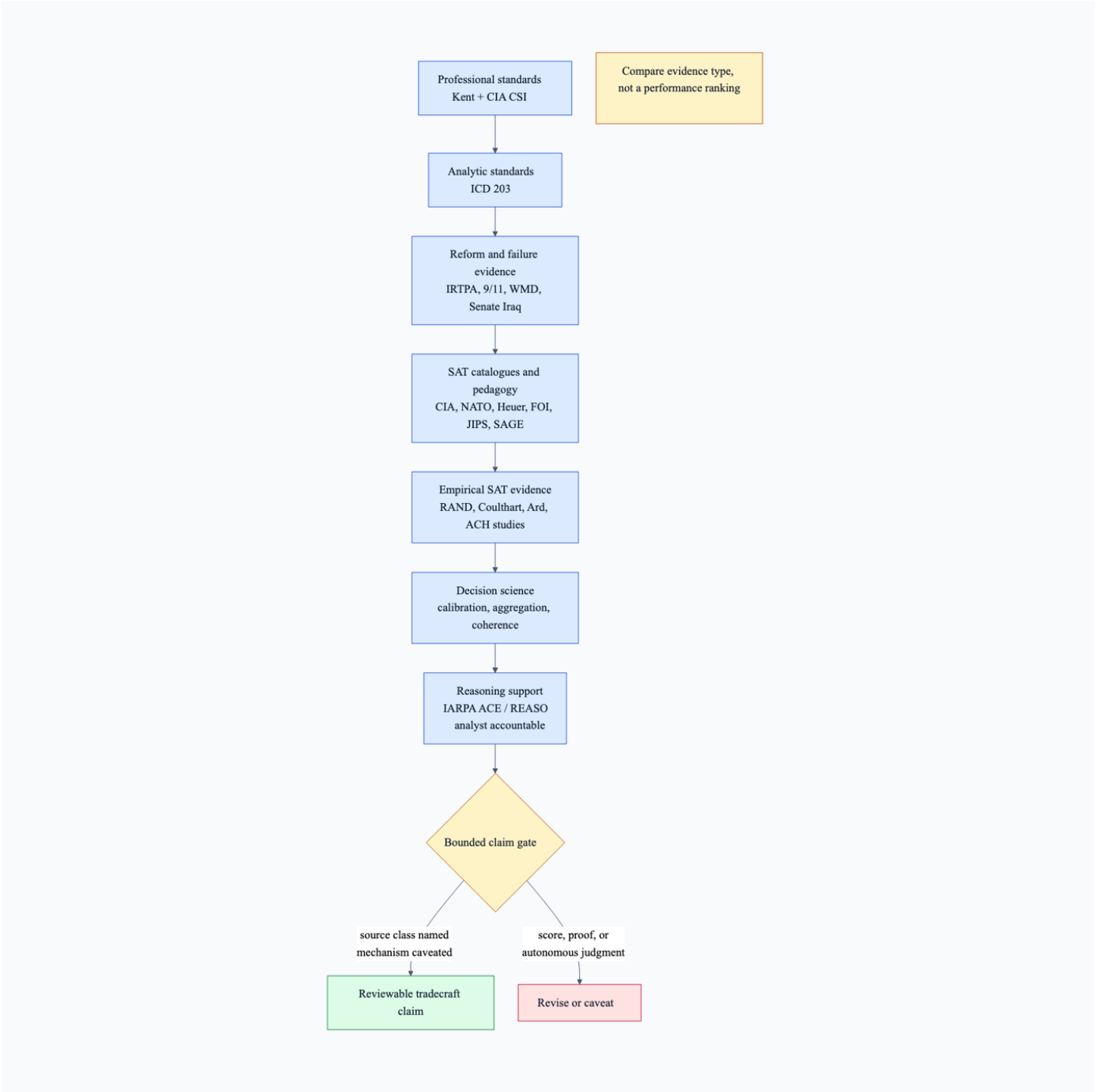


Figure 121: Source-backed conceptual schematic comparing the source classes behind analytic-tradecraft claims: professional standards, official reform and postmortems, SAT catalogues, empirical SAT studies, forecasting calibration, and AI reasoning-support programs. The denominator is AGEINT's curated analytic-tradecraft anchor set, and the figure fails closed when doctrine, adoption, or postmortem pressure becomes an empirical accuracy score or universal debiasing overclaim.

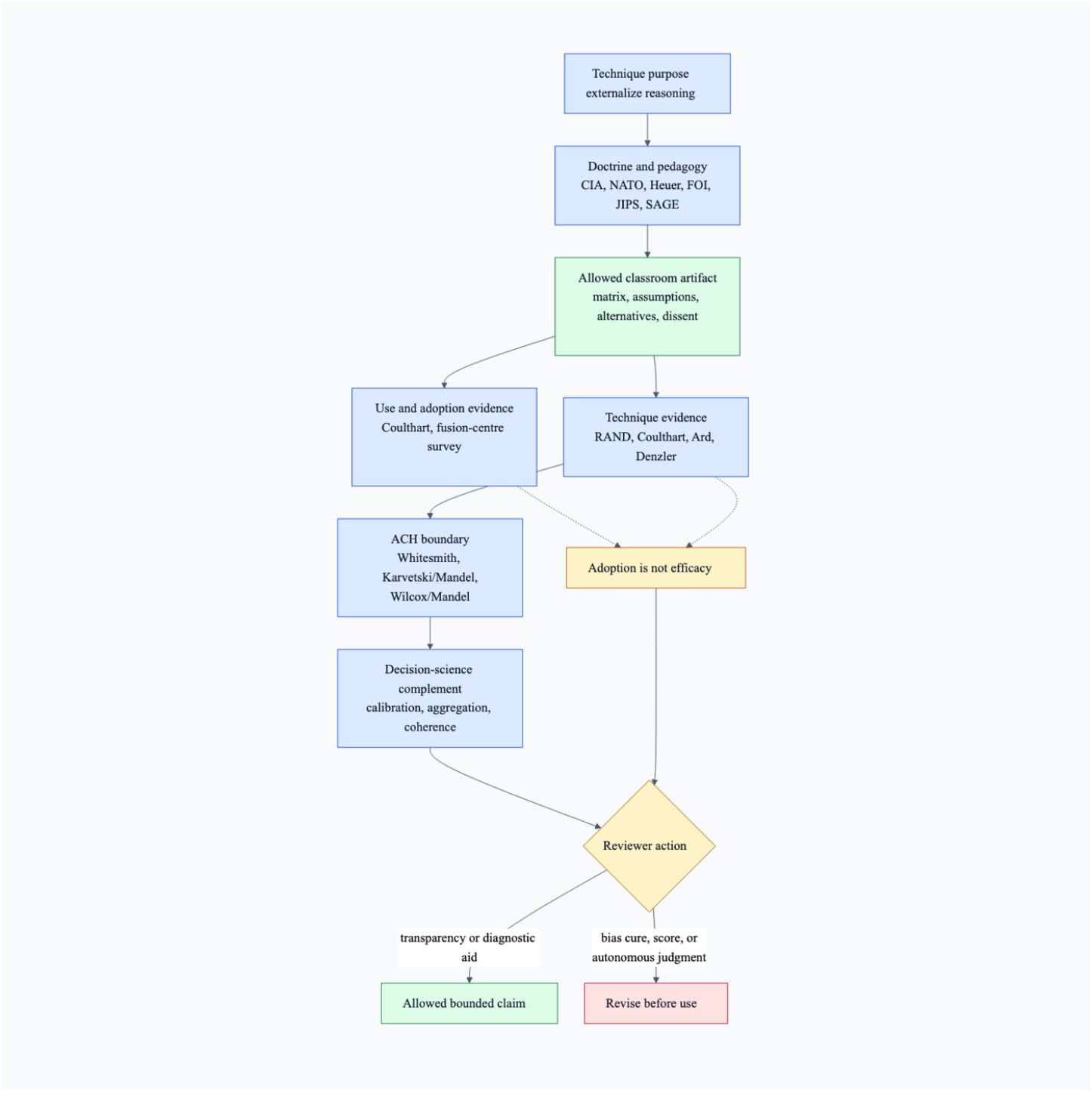


Figure 122: Source-backed conceptual schematic comparing SAT purpose, doctrine, classroom artifacts, adoption studies, technique-specific experiments, ACH critiques, and decision-science complements. The local artifact set is the chapter 41 SAT lesson and its curated anchors; the figure fails closed on overclaim language that treats SATs as a proven universal bias remedy, an empirical score, or a replacement for analyst accountability.

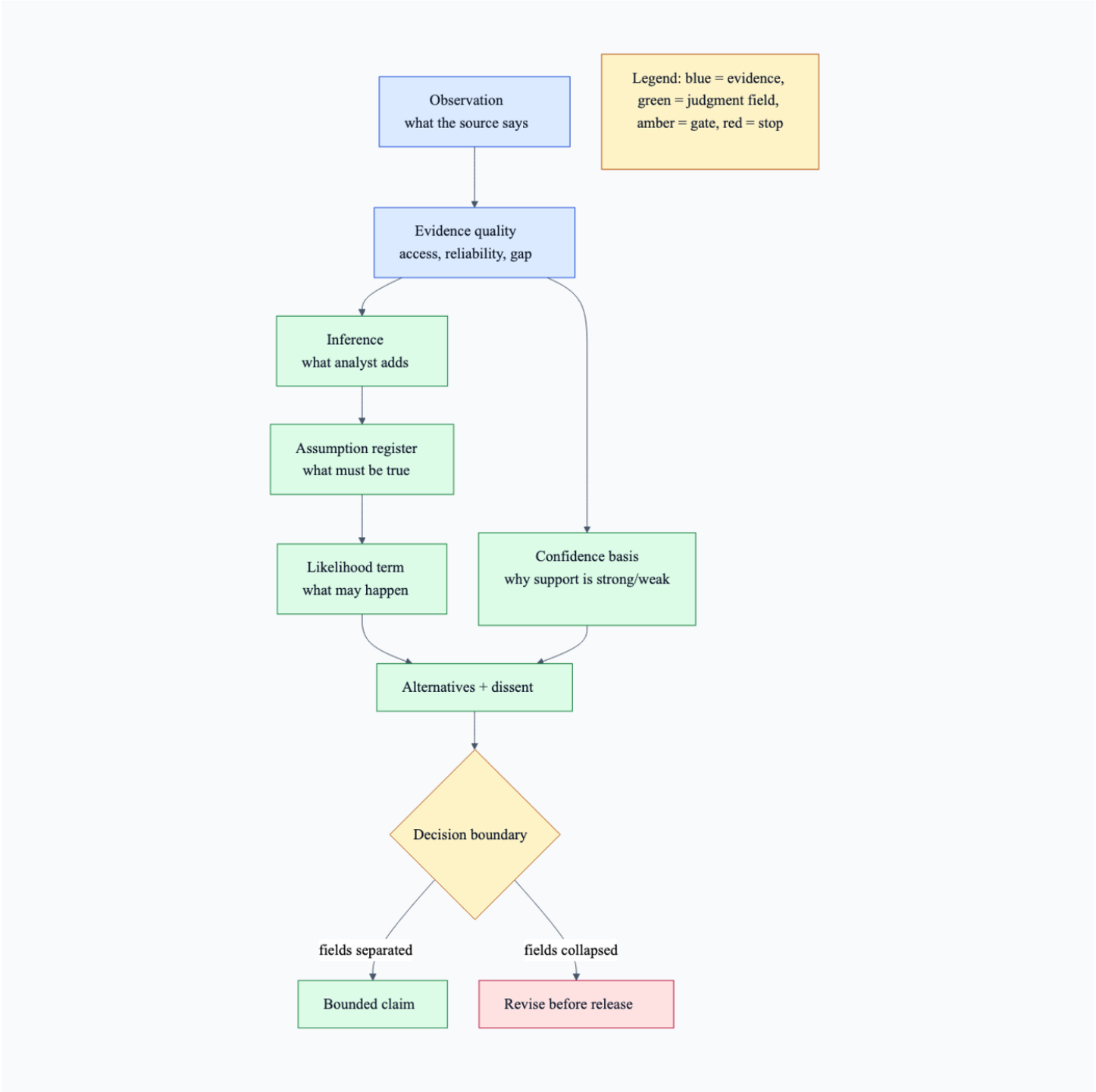


Figure 123: Source-backed conceptual schematic decomposing analytic tradecraft claims while separating observation, inference, assumption, likelihood, confidence, dissent, and decision-boundary fields before any manuscript claim is treated as reviewable. Its reader value is to make Observation what the source says, Evidence quality access, reliability, gap, Inference what analyst adds, and Assumption register what must be true visible at a glance, with the epistemic rigor and analytic tradecraft / structured analytic techniques sats section as the source section and defensive review as the boundary.

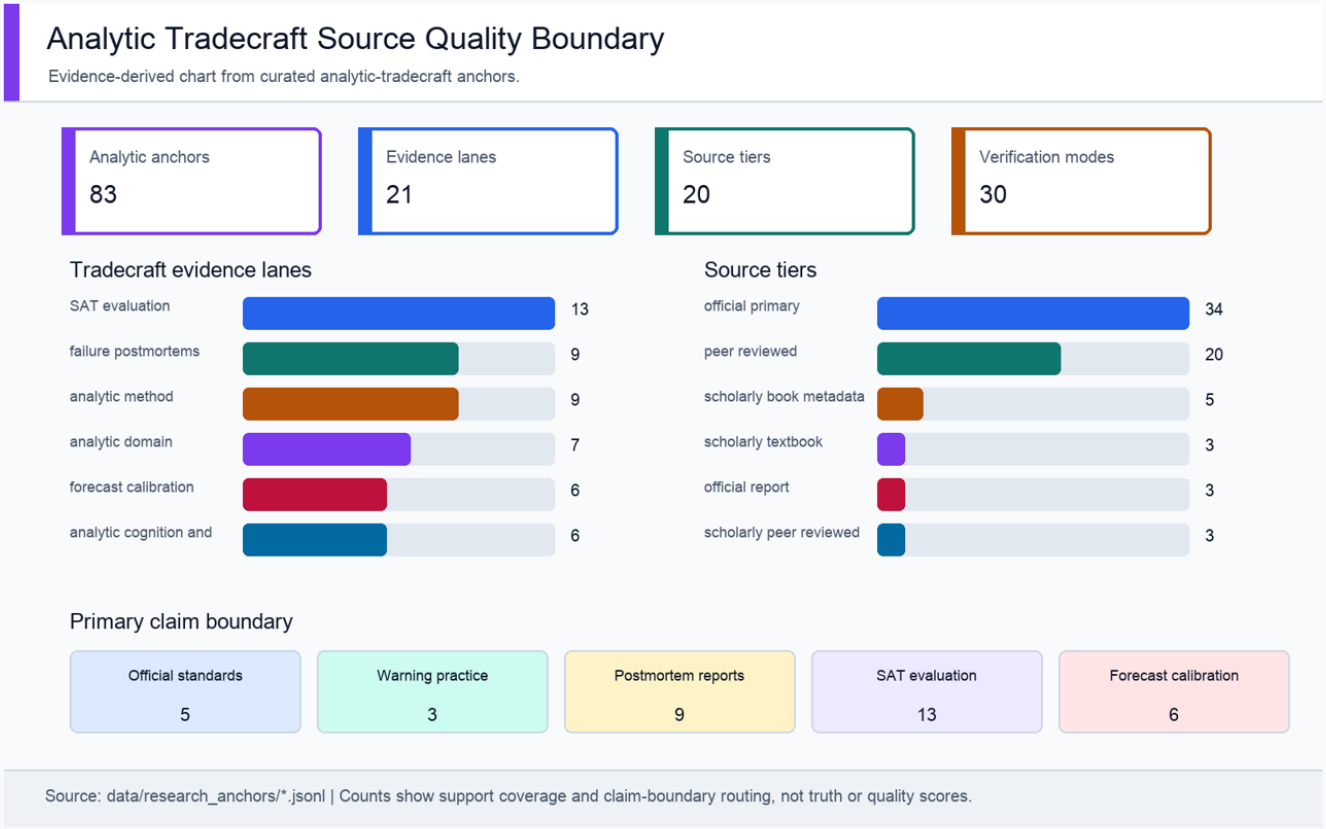


Figure 124: Source-backed evidence-derived chart from local research-anchor metadata showing official, standards, statutory, postmortem, scholarly evaluation, and forecasting evidence lanes for analytic-tradecraft claims. The captioned view belongs to the epistemic rigor and analytic tradecraft / structured analytic techniques sats section and should be read as a map of analytic source quality boundary categories, denominators, evidence lanes, limitations, and reviewer-use cautions, not as a capability score or live-task instruction.

57.2 Structured-Judgment Lens path for Structured Analytic Techniques (SATs): lesson cluster, safe artifact, and review

Evidence anchor. Section 57; [237, 2026].

57.2.1 Structured Analytic Techniques (SATs) practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 57; [237, 2026].

57.2.2 Structured Analytic Techniques (SATs) topic lessons: source-backed concepts and transfer tasks

This module builds analytic tradecraft as disciplined judgment under uncertainty: claims become useful only when evidence, assumptions, alternatives, confidence, and dissent remain visible. The sequence opens with **CIA Tradecraft Primer: SATs for Intelligence Analysis**, **ICD 203 Analytic Standards: The Nine Tradecraft Standards**, **Psychology of Intelligence Analysis (Heuer, CIA 1999)** and applies the **Structured-Judgment Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 116; module overview Section 57; curriculum atlas Section 2.

Triangulation anchors. In module 41's topic-lessons section, directly verified anchors for the **Analytic Tradecraft and Source Integrity** lane include [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2026e]; [Agency, 2009]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

57.2.2.1 Lesson 1: CIA Tradecraft Primer: SATs for Intelligence Analysis **Concept. CIA Tradecraft Primer: SATs for Intelligence Analysis** studies the declassified record for institutional lessons about oversight, source protection, and limits on translating history into practice.

Why it matters. Without explicit treatment of **CIA Tradecraft Primer**, collapsing reporting, inference, and judgment into one line undermines structured reasoning and source-integrity review; the lesson builds the habit to separate reporting from inference, and inference from judgment.

Source support. CIA Tradecraft Primer: SATs for Intelligence Analysis rests on [189, 2026]. Its anchor reference records: This primer will assist analysts in dealing with the perennial problems of intelligence. Use it for the working definition that **CIA Tradecraft Primer: SATs for Intelligence Analysis** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. For **CIA Tradecraft Primer**, reason from the sources cited in this row. [189, 2026] This primer will assist analysts in dealing with the perennial problems of intelligence. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **CIA Tradecraft Primer**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must separate the source descriptor, the bounded judgment about **CIA Tradecraft Primer**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape **CIA Tradecraft Primer** work as a **competing-hypotheses evidence table** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **CIA Tradecraft Primer**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. Reuse the **CIA Tradecraft Primer** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

57.2.2.2 Lesson 2: ICD 203 Analytic Standards: The Nine Tradecraft Standards **Concept. ICD 203 Analytic Standards: The Nine Tradecraft Standards** — Calibrate confidence to evidence strength, source quality, and alternative explanations—not to rhetorical certainty.

Why it matters. Analysts use **ICD 203 Analytic Standards** to separate reporting from inference, and inference from judgment. A defensible treatment names the judgment it enables for structured reasoning and source-integrity review, the proof limit that collapsing reporting, inference, and judgment into one line would otherwise hide, and the reviewer accountable for challenge.

Source support. ICD 203 Analytic Standards: The Nine Tradecraft Standards rests on [002, 2026] and [190, 2026]. The closest source to this row notes: Intelligence Community's public site, presenting objectivity as a core IC value. Use them for pinning down the scope of **ICD 203 Analytic Standards: The Nine Tradecraft Standards**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. Ground **ICD 203 Analytic Standards** in the evidence the row cites. [002, 2026] ICD 203 directs the heads of IC elements to designate a similar individual or office to respond. [190, 2026] A page on Intelligence.gov, the U.S. Intelligence Community's public site, presenting objectivity as a core IC value. It explains that intelligence analysis must be performed and conveyed without distortion from personal or political bias, and references the standards codified in Intelligence Community Directive (ICD) 203 on analytic standards. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **ICD 203 Analytic Standards**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must separate the source descriptor, the bounded judgment about **ICD 203 Analytic Standards**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape **ICD 203 Analytic Standards** work as a **competing-hypotheses evidence table** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **ICD 203 Analytic Standards**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. Reuse the **ICD 203 Analytic Standards** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

57.2.2.3 Lesson 3: Psychology of Intelligence Analysis (Heuer, CIA 1999) **Concept. Psychology of Intelligence Analysis (Heuer, CIA 1999)** studies the declassified record for institutional lessons about oversight, source protection, and limits on translating history into practice.

Why it matters. Without explicit treatment of **Psychology of Intelligence Analysis (Heuer, CIA 1999)**, collapsing reporting, inference, and judgment into one line undermines structured reasoning and source-integrity review; the lesson builds the habit to separate reporting from inference, and inference from judgment.

Source support. Psychology of Intelligence Analysis (Heuer, CIA 1999) uses curated analytic-tradecraft anchors [of the Director of National Intelligence, 2015]; [Agency, 2009]; [for the Study of Intelligence, 2002]; [Cooper, 2005]; [Johnston, 2005]; [on Terrorist Attacks Upon the United States, 2004]; [on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005]; [on Intelligence, 2004]; [Bruce, 2016]; [Coulthart, 2017]; [Tetlock, 2018]; [et al., 2019]; [Whitesmith, 2019]; [Mandel, 2020]; [Mandel, 2024]; [Barnes and Mandel, 2014]; [Tetlock, 2015b]; [Activity, 2010]; [Activity, 2023]; [McMahon, 2024]. The inherited guide citation(s) [180, 2026]; [191, 2026]; [192, 2026] remain context only; primary support must keep likelihood, confidence, assumptions, alternatives, dissent, source quality, ACH limits, and refresh duty separate. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. For **Psychology of Intelligence Analysis (Heuer, CIA 1999)**, use the curated analytic-tradecraft anchors [of the Director of National Intelligence, 2015]; [Agency, 2009]; [for the Study of Intelligence, 2002]; [Cooper, 2005]; [Johnston, 2005]; [on Terrorist Attacks Upon the United States, 2004]; [on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005]; [on Intelligence, 2004]; [Bruce, 2016]; [Coulthart, 2017]; [Tetlock, 2018]; [et al., 2019]; [Whitesmith, 2019]; [Mandel, 2020]; [Mandel, 2024]; [Barnes and Mandel, 2014]; [Tetlock, 2015b]; [Activity, 2010]; [Activity, 2023]; [McMahon, 2024]. Pull observation, inference, assumption, likelihood, confidence, dissent, decision-uptake boundary, postmortem learning, and the empirical limit that would force a weaker claim. Treat SATs as reviewable reasoning artifacts, not validated universal debiasing or autonomous judgment replacements.

Student artifact. For **Psychology of Intelligence Analysis (Heuer, CIA 1999)**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must separate the source descriptor, the bounded judgment about **Psychology of Intelligence Analysis**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape the same topic work as a **competing-hypotheses evidence table** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Psychology of Intelligence Analysis (Heuer, CIA 1999)**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. Apply this module's safe boundary for **Psychology of Intelligence Analysis (Heuer, CIA 1999)** to another artifact while keeping structured reasoning and source-integrity review and reviewer ownership explicit.

57.2.2.4 Lesson 4: Structured Analytic Techniques (Heuer & Pherson, 2011)

Concept. Structured Analytic Techniques (Heuer & Pherson, 2011) uses the method to keep alternatives, disconfirming evidence, and confidence visible.

Why it matters. Analysts use **Structured Analytic Techniques (Heuer & Pherson, 2011)** to separate reporting from inference, and inference from judgment. A defensible treatment names the judgment it enables for structured reasoning and source-integrity review, the proof limit that collapsing reporting, inference, and judgment into one line would otherwise hide, and the reviewer accountable for challenge.

Source support. Structured Analytic Techniques (Heuer & Pherson, 2011) uses curated analytic-tradecraft anchors [of the Director of National Intelligence, 2015]; [Agency, 2009]; [for the Study of Intelligence, 2002]; [Cooper, 2005]; [Johnston, 2005]; [on Terrorist Attacks Upon the United States, 2004]; [on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005]; [on Intelligence, 2004]; [Bruce, 2016]; [Coulthart, 2017]; [Tetlock, 2018]; [et al., 2019]; [Whitesmith, 2019]; [Mandel, 2020]; [Mandel, 2024]; [Barnes and Mandel, 2014]; [Tetlock, 2015b]; [Activity, 2010]; [Activity, 2023]; [McMahon, 2024]. The inherited guide citation(s) [193, 2026]; [194, 2026] remain context only; primary support must keep likelihood, confidence, assumptions, alternatives, dissent, source quality, ACH limits, and refresh duty separate. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. For **Structured Analytic Techniques (Heuer & Pherson, 2011)**, use the curated analytic-tradecraft anchors [of the Director of National Intelligence, 2015]; [Agency, 2009]; [for the Study of Intelligence, 2002]; [Cooper, 2005]; [Johnston, 2005]; [on Terrorist Attacks Upon the United States, 2004]; [on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005]; [on Intelligence, 2004]; [Bruce, 2016]; [Coulthart, 2017]; [Tetlock, 2018]; [et al., 2019]; [Whitesmith, 2019]; [Mandel, 2020]; [Mandel, 2024]; [Barnes and Mandel, 2014]; [Tetlock, 2015b]; [Activity, 2010]; [Activity, 2023]; [McMahon, 2024]. Pull observation, inference, assumption, likelihood, confidence, dissent, decision-uptake boundary, postmortem learning, and the empirical limit that would force a weaker claim. Treat SATs as reviewable reasoning artifacts, not validated universal debiasing or autonomous judgment replacements.

Student artifact. For **Structured Analytic Techniques (Heuer & Pherson, 2011)**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must separate the source descriptor, the bounded judgment about **Structured Analytic Techniques**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape the same topic work as a **competing-hypotheses evidence table** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Structured Analytic Techniques (Heuer & Pherson, 2011)**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. Transfer **Structured Analytic Techniques (Heuer & Pherson, 2011)** from this module to a second motif by preserving structured reasoning and source-integrity review, replacing action with audit, and naming the blocked use.

57.2.2.5 Lesson 5: Analysis of Competing Hypotheses (ACH)

Concept. Analysis of Competing Hypotheses (ACH) uses the method to keep alternatives, disconfirming evidence, and confidence visible.

Why it matters. Analysis of Competing Hypotheses (ACH) matters in the **Analytic Tradecraft and Source Integrity** lane because structured reasoning and source-integrity evidence must stay separate from judgment; collapsing reporting, inference, and judgment into one line is a common failure.

Source support. Analysis of Competing Hypotheses (ACH) rests on [297, 2026] and [298, 2026]. The lead source's own note reads: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for pinning down the scope of **Analysis of Competing Hypotheses (ACH)**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. For **Analysis of Competing Hypotheses (ACH)**, work from the cited evidence behind this row. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Analysis of Competing Hypotheses (ACH)**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must separate the source descriptor, the bounded judgment about **Analysis of Competing Hypotheses**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape this subject work as a **competing-hypotheses evidence table** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Analysis of Competing Hypotheses (ACH)**: that listing one favored hypothesis is enough without testing alternatives.

Transfer task. Transfer **Analysis of Competing Hypotheses (ACH)** from this module to a second motif by preserving structured reasoning and source-integrity review, replacing action with audit, and naming the blocked use.

Diagnosticity ratio. The diagnosticity an ACH table scores is a likelihood ratio. For two hypotheses H_i, H_j and an item of evidence E, the posterior odds update as

$$\frac{P(H_i \mid E)}{P(H_j \mid E)} = \frac{P(E \mid H_i)}{P(E \mid H_j)} \times \frac{P(H_i)}{P(H_j)}.$$

Evidence is diagnostic only when the likelihood ratio $P(E \mid H_i)/P(E \mid H_j)$ departs from 1; evidence consistent with every hypothesis (ratio ≈ 1) carries no diagnostic weight, which is exactly Heuer's rule to weigh disconfirming evidence over confirming evidence [192, 2026]; [297, 2026].

57.2.2.6 Lesson 6: Devil's Advocacy and Red Teaming **Concept. Devil's Advocacy and Red Teaming** structures evaluation as misuse-case testing with blocked outcomes, logged evidence, and reviewer disposition.

Why it matters. Analysts use **Devil's Advocacy** to separate reporting from inference, and inference from judgment. A defensible treatment names the judgment it enables for structured reasoning and source-integrity review, the proof limit that collapsing reporting, inference, and judgment into one line would otherwise hide, and the reviewer accountable for challenge.

Source support. Devil's Advocacy and Red Teaming rests on [300, 2026], [304, 2026], and [306, 2026]. The lead source's own note reads: NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Use them for pinning down the scope of **Devil's Advocacy and Red Teaming**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. For **Devil's Advocacy**, work from the cited evidence behind this row. [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. Build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must separate the source descriptor, the bounded judgment about **Devil's Advocacy**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape this subject work as a **competing-hypotheses evidence table** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Devil's Advocacy**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. Apply this module's safe boundary for **Devil's Advocacy** to another artifact while keeping structured reasoning and source-integrity review and reviewer ownership explicit.

57.2.2.7 Lesson 7: Alternative Futures Analysis **Concept. Alternative Futures Analysis** uses structured ideation to widen alternatives before converging on evidence-tested judgments.

Why it matters. Alternative Futures Analysis matters in the **Analytic Tradecraft and Source Integrity** lane because structured reasoning and source-integrity evidence must stay separate from judgment; collapsing reporting, inference, and judgment into one line is a common failure.

Source support. Alternative Futures Analysis rests on [297, 2026] and [298, 2026]. Its anchor reference records: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for the claim that **Alternative Futures Analysis** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. Read **Alternative Futures Analysis** against the works cited for this row. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. Build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must separate the source descriptor, the bounded judgment about **Alternative Futures Analysis**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape this subject work as a **competing-hypotheses evidence table** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Alternative Futures Analysis**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. Reuse the **Alternative Futures Analysis** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

57.2.2.8 Lesson 8: Brainstorming and Divergent Thinking Techniques **Concept. Brainstorming and Divergent Thinking Techniques** uses structured ideation to widen alternatives before converging on evidence-tested judgments.

Why it matters. Brainstorming and Divergent Thinking Techniques connects classroom vocabulary to Analytic Tradecraft and Source Integrity practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Brainstorming and Divergent Thinking Techniques rests on [297, 2026] and [298, 2026]. Its anchor reference records: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for the claim that **Brainstorming and Divergent Thinking Techniques** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. Ground **Brainstorming and Divergent Thinking Techniques** in the evidence the row cites. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. Build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must separate the source descriptor, the bounded judgment about **Brainstorming and Divergent Thinking Techniques**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape this subject work as a **competing-hypotheses evidence table** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Brainstorming and Divergent Thinking Techniques**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. Transfer **Brainstorming and Divergent Thinking Techniques** from this module to a second motif by preserving structured reasoning and source-integrity review, replacing action with audit, and naming the blocked use.

57.2.2.9 Lesson 9: Deception Detection SATs **Concept. Deception Detection SATs** compares deception indicators with alternative explanations and uncertainty before any operational inference.

Why it matters. Without explicit treatment of **Deception Detection SATs**, collapsing reporting, inference, and judgment into one line undermines structured reasoning and source-integrity review; the lesson builds the habit to separate reporting from inference, and inference from judgment.

Source support. Deception Detection SATs uses curated analytic-tradecraft anchors [of the Director of National Intelligence, 2015]; [Agency, 2009]; [for the Study of Intelligence, 2002]; [Cooper, 2005]; [Johnston, 2005]; [on Terrorist Attacks Upon the United States, 2004]; [on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005]; [on Intelligence, 2004]; [Bruce, 2016]; [Coulthart, 2017]; [Tetlock, 2018]; [et al., 2019]; [Whitesmith, 2019]; [Mandel, 2020]; [Mandel, 2024]; [Barnes and Mandel, 2014]; [Tetlock, 2015b]; [Activity, 2010]; [Activity, 2023]; [McMahon, 2024]. The inherited guide citation(s) [193, 2026] remain context only; primary support must keep likelihood, confidence, assumptions, alternatives, dissent, source quality, ACH limits, and refresh duty separate. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. For **Deception Detection SATs**, use the curated analytic-tradecraft anchors [of the Director of National Intelligence, 2015]; [Agency, 2009]; [for the Study of Intelligence, 2002]; [Cooper, 2005]; [Johnston, 2005]; [on Terrorist Attacks Upon the United States, 2004]; [on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005]; [on Intelligence, 2004]; [Bruce, 2016]; [Coulthart, 2017]; [Tetlock, 2018]; [et al., 2019]; [Whitesmith, 2019]; [Mandel, 2020]; [Mandel, 2024]; [Barnes and Mandel, 2014]; [Tetlock, 2015b]; [Activity, 2010]; [Activity, 2023]; [McMahon, 2024]. Pull observation, inference, assumption, likelihood, confidence, dissent, decision-uptake boundary, postmortem learning, and the empirical limit that would force a weaker claim. Treat SATs as reviewable reasoning artifacts, not validated universal debiasing or autonomous judgment replacements.

Student artifact. For **Deception Detection SATs**, build a threat-model review card with assumptions, disconfirming evidence, and confidence language. Shape the same topic work as a **competing-hypotheses evidence table** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Deception Detection SATs**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. Transfer **Deception Detection SATs** from this module to a second motif by preserving structured reasoning and source-integrity review, replacing action with audit, and naming the blocked use.

57.2.2.10 Lesson 10: Key Assumptions Check **Concept. Key Assumptions Check** — List assumptions explicitly and test which ones would change the judgment if falsified.

Why it matters. Without explicit treatment of **Key Assumptions Check**, collapsing reporting, inference, and judgment into one line undermines structured reasoning and source-integrity review; the lesson builds the habit to separate reporting from inference, and inference from judgment.

Source support. Key Assumptions Check rests on [297, 2026] and [298, 2026]. The closest source to this row notes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for fixing what **Key Assumptions Check** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. Ground **Key Assumptions Check** in the evidence the row cites. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. Build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must separate the source descriptor, the bounded judgment about **Key Assumptions Check**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape this subject work as a **competing-hypotheses evidence table** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Key Assumptions Check**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. Apply this module's safe boundary for **Key Assumptions Check** to another artifact while keeping structured reasoning and source-integrity review and reviewer ownership explicit.

57.2.2.11 Lesson 11: Indicators Validator **Concept. Indicators Validator** applies structured analytic methods with explicit alternatives, evidence tables, and calibrated confidence—not rhetorical certainty.

Why it matters. Indicators Validator connects classroom vocabulary to Analytic Tradecraft and Source Integrity practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Indicators Validator rests on [309, 2026], [310, 2026], and [300, 2026]. The lead source's own note reads: It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). Use them for the working definition that **Indicators Validator** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. For **Indicators Validator**, work from the cited evidence behind this row. [309, 2026] An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection. [310, 2026] The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. Build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must separate the source descriptor, the bounded judgment about **Indicators Validator**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape this subject work as a **competing-hypotheses evidence table** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Indicators Validator**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. Apply this module's safe boundary for **Indicators Validator** to another artifact while keeping structured reasoning and source-integrity review and reviewer ownership explicit.

57.2.2.12 Lesson 12: What If? / Pre-Mortem Analysis **Concept. What If? / Pre-Mortem Analysis** applies structured analytic methods with explicit alternatives, evidence tables, and calibrated confidence—not rhetorical certainty.

Why it matters. What If? / Pre-Mortem Analysis matters in the **Analytic Tradecraft and Source Integrity** lane because structured reasoning and source-integrity evidence must stay separate from judgment; collapsing reporting, inference, and judgment into one line is a common failure.

Source support. What If? / Pre-Mortem Analysis rests on [297, 2026] and [298, 2026]. Its anchor reference records: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for pinning down the scope of **What If? / Pre-Mortem Analysis**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. Read **What If? / Pre-Mortem Analysis** against the works cited for this row. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **What If? / Pre-Mortem Analysis**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must separate the source descriptor, the bounded judgment about **What If Pre-Mortem Analysis**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape this subject work as a **competing-hypotheses evidence table** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **What If? / Pre-Mortem Analysis**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. Reuse the **What If? / Pre-Mortem Analysis** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

57.2.2.13 Lesson 13: Analytic Tradecraft and the Intelligence Community (Tandfonline, 2014)

Concept. Analytic Tradecraft and the Intelligence Community (Tandfonline, 2014) maps the theory to institutions: priorities, feedback, incentives, review loops, and records shape what an intelligence community notices and ignores.

Why it matters. Analytic Tradecraft connects classroom vocabulary to Analytic Tradecraft and Source Integrity practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Analytic Tradecraft and the Intelligence Community (Tandfonline, 2014) uses curated analytic-tradecraft anchors [of the Director of National Intelligence, 2015]; [Agency, 2009]; [for the Study of Intelligence, 2002]; [Cooper, 2005]; [Johnston, 2005]; [on Terrorist Attacks Upon the United States, 2004]; [on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005]; [on Intelligence, 2004]; [Bruce, 2016]; [Coulthart, 2017]; [Tetlock, 2018]; [et al., 2019]; [Whitesmith, 2019]; [Mandel, 2020]; [Mandel, 2024]; [Barnes and Mandel, 2014]; [Tetlock, 2015b]; [Activity, 2010]; [Activity, 2023]; [McMahon, 2024]. The inherited guide citation(s) [195, 2026] remain context only; primary support must keep likelihood, confidence, assumptions, alternatives, dissent, source quality, ACH limits, and refresh duty separate. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. For **Analytic Tradecraft**, use the curated analytic-tradecraft anchors [of the Director of National Intelligence, 2015]; [Agency, 2009]; [for the Study of Intelligence, 2002]; [Cooper, 2005]; [Johnston, 2005]; [on Terrorist Attacks Upon the United States, 2004]; [on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005]; [on Intelligence, 2004]; [Bruce, 2016]; [Coulthart, 2017]; [Tetlock, 2018]; [et al., 2019]; [Whitesmith, 2019]; [Mandel, 2020]; [Mandel, 2024]; [Barnes and Mandel, 2014]; [Tetlock, 2015b]; [Activity, 2010]; [Activity, 2023]; [McMahon, 2024]. Pull observation, inference, assumption, likelihood, confidence, dissent, decision-uptake boundary, postmortem learning, and the empirical limit that would force a weaker claim. Treat SATs as reviewable reasoning artifacts, not validated universal debiasing or autonomous judgment replacements.

Student artifact. For **Analytic Tradecraft**, build an institutional feedback-loop map with incentives, review points, and oversight hooks. Shape **Analytic Tradecraft** work as a **competing-hypotheses evidence table** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Analytic Tradecraft**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. Transfer **Analytic Tradecraft** from this module to a second motif by preserving structured reasoning and source-integrity review, replacing action with audit, and naming the blocked use.

57.2.2.14 Lesson 14: Analytic Tradecraft Standards in Army Intelligence

Concept. Analytic Tradecraft Standards in Army Intelligence applies ICD 203 tradecraft standards: sourcing, uncertainty, distinctions, alternatives, relevance, argumentation, consistency, accuracy, and visuals.

Why it matters. Analytic Tradecraft Standards matters in the **Analytic Tradecraft and Source Integrity** lane because structured reasoning and source-integrity evidence must stay separate from judgment; collapsing reporting, inference, and judgment into one line is a common failure.

Source support. Analytic Tradecraft Standards in Army Intelligence uses curated analytic-tradecraft anchors [of the Director of National Intelligence, 2015]; [Agency, 2009]; [for the Study of Intelligence, 2002]; [Cooper, 2005]; [Johnston, 2005]; [on Terrorist Attacks Upon the United States, 2004]; [on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005]; [on Intelligence, 2004]; [Bruce, 2016]; [Coulthart, 2017]; [Tetlock, 2018]; [et al., 2019]; [Whitesmith, 2019]; [Mandel, 2020]; [Mandel, 2024]; [Barnes and Mandel, 2014]; [Tetlock, 2015b]; [Activity, 2010]; [Activity, 2023]; [McMahon, 2024]. The inherited guide citation(s) [196, 2026] remain context only; primary support must keep likelihood, confidence, assumptions, alternatives, dissent, source quality, ACH limits, and refresh duty separate. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. For **Analytic Tradecraft Standards**, use the curated analytic-tradecraft anchors [of the Director of National Intelligence, 2015]; [Agency, 2009]; [for the Study of Intelligence, 2002]; [Cooper, 2005]; [Johnston, 2005]; [on Terrorist Attacks Upon the United States, 2004]; [on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005]; [on Intelligence, 2004]; [Bruce, 2016]; [Coulthart, 2017]; [Tetlock, 2018]; [et al., 2019]; [Whitesmith, 2019]; [Mandel, 2020]; [Mandel, 2024]; [Barnes and Mandel, 2014]; [Tetlock, 2015b]; [Activity, 2010]; [Activity, 2023]; [McMahon, 2024]. Pull observation, inference, assumption, likelihood, confidence, dissent, decision-uptake boundary, postmortem learning, and the empirical limit that would force a weaker claim. Treat SATs as reviewable reasoning artifacts, not validated universal debiasing or autonomous judgment replacements.

Student artifact. For **Analytic Tradecraft Standards**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must separate the source descriptor, the bounded judgment about **Analytic Tradecraft Standards in Army**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape **Analytic Tradecraft Standards** work as a **competing-hypotheses evidence table** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Analytic Tradecraft Standards**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. Transfer **Analytic Tradecraft Standards** from this module to a second motif by preserving structured reasoning and source-integrity review, replacing action with audit, and naming the blocked use.

57.2.2.15 Lesson 15: Cognitive Biases: Confirmation Bias, Anchoring, Groupthink in Intelligence

Concept. Cognitive Biases: Confirmation Bias, Anchoring, Groupthink in Intelligence connects cognitive bias literacy to review checkpoints, dissent channels, and explicit uncertainty language.

Why it matters. Analysts use **Cognitive Biases** to separate reporting from inference, and inference from judgment. A defensible treatment names the judgment it enables for structured reasoning and source-integrity review, the proof limit that collapsing reporting, inference, and judgment into one line would otherwise hide, and the reviewer accountable for challenge.

Source support. Cognitive Biases: Confirmation Bias, Anchoring, Groupthink in Intelligence uses curated analytic-tradecraft anchors [of the Director of National Intelligence, 2015]; [Agency, 2009]; [for the Study of Intelligence, 2002]; [Cooper, 2005]; [Johnston, 2005]; [on Terrorist Attacks Upon the United States, 2004]; [on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005]; [on Intelligence, 2004]; [Bruce, 2016]; [Coulthart, 2017]; [Tetlock, 2018]; [et al., 2019]; [Whitesmith, 2019]; [Mandel, 2020]; [Mandel, 2024]; [Barnes and Mandel, 2014]; [Tetlock, 2015b]; [Activity, 2010]; [Activity, 2023]; [McMahon, 2024]. The inherited guide citation(s) [180, 2026] remain context only; primary support must keep likelihood, confidence, assumptions, alternatives, dissent, source quality, ACH limits, and refresh duty separate. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. For **Cognitive Biases**, use the curated analytic-tradecraft anchors [of the Director of National Intelligence, 2015]; [Agency, 2009]; [for the Study of Intelligence, 2002]; [Cooper, 2005]; [Johnston, 2005]; [on Terrorist Attacks Upon the United States, 2004]; [on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005]; [on Intelligence, 2004]; [Bruce, 2016]; [Coulthart, 2017]; [Tetlock, 2018]; [et al., 2019]; [Whitesmith, 2019]; [Mandel, 2020]; [Mandel, 2024]; [Barnes and Mandel, 2014]; [Tetlock, 2015b]; [Activity, 2010]; [Activity, 2023]; [McMahon, 2024]. Pull observation, inference, assumption, likelihood, confidence, dissent, decision-uptake boundary, postmortem learning, and the empirical limit that would force a weaker claim. Treat SATs as reviewable reasoning artifacts, not validated universal debiasing or autonomous judgment replacements.

Student artifact. For **Cognitive Biases**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must separate the source descriptor, the bounded judgment about **Cognitive Biases**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape **Cognitive Biases** work as a **competing-hypotheses evidence table** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Cognitive Biases**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. Reuse the **Cognitive Biases** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

57.2.2.16 Lesson 16: From Spycraft to Self-Mastery: SATs for Everyday Decision-Making Concept. From Spycraft to Self-Mastery: SATs for Everyday Decision-Making

applies structured analytic methods with explicit alternatives, evidence tables, and calibrated confidence—not rhetorical certainty.

Why it matters. Without explicit treatment of **From Spycraft to Self-Mastery**, collapsing reporting, inference, and judgment into one line undermines structured reasoning and source-integrity review; the lesson builds the habit to separate reporting from inference, and inference from judgment.

Source support. From Spycraft to Self-Mastery: SATs for Everyday Decision-Making uses curated analytic-tradecraft anchors [of the Director of National Intelligence, 2015]; [Agency, 2009]; [for the Study of Intelligence, 2002]; [Cooper, 2005]; [Johnston, 2005]; [on Terrorist Attacks Upon the United States, 2004]; [on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005]; [on Intelligence, 2004]; [Bruce, 2016]; [Coulthart, 2017]; [Tetlock, 2018]; [et al., 2019]; [Whitesmith, 2019]; [Mandel, 2020]; [Mandel, 2024]; [Barnes and Mandel, 2014]; [Tetlock, 2015b]; [Activity, 2010]; [Activity, 2023]; [McMahon, 2024]. The inherited guide citation(s) [188, 2026] remain context only; primary support must keep likelihood, confidence, assumptions, alternatives, dissent, source quality, ACH limits, and refresh duty separate. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. For **From Spycraft to Self-Mastery**, use the curated analytic-tradecraft anchors [of the Director of National Intelligence, 2015]; [Agency, 2009]; [for the Study of Intelligence, 2002]; [Cooper, 2005]; [Johnston, 2005]; [on Terrorist Attacks Upon the United States, 2004]; [on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005]; [on Intelligence, 2004]; [Bruce, 2016]; [Coulthart, 2017]; [Tetlock, 2018]; [et al., 2019]; [Whitesmith, 2019]; [Mandel, 2020]; [Mandel, 2024]; [Barnes and Mandel, 2014]; [Tetlock, 2015b]; [Activity, 2010]; [Activity, 2023]; [McMahon, 2024]. Pull observation, inference, assumption, likelihood, confidence, dissent, decision-uptake boundary, postmortem learning, and the empirical limit that would force a weaker claim. Treat SATs as reviewable reasoning artifacts, not validated universal debiasing or autonomous judgment replacements.

Student artifact. For **From Spycraft to Self-Mastery**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must separate the source descriptor, the bounded judgment about **Spycraft to Self-Mastery**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape **From Spycraft to Self-Mastery** work as a **competing-hypotheses evidence table** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **From Spycraft to Self-Mastery**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. Reuse the **From Spycraft to Self-Mastery** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

57.2.3 Structured Analytic Techniques (SATs) worked safe example: synthetic inputs, evidence, and review

Worked example: a synthetic analyst cell evaluates whether a benign supplier delay signals normal friction or elevated risk. [237, 2026]; [266, 2026].

Triangulation anchors. In module 41's worked-example section, directly verified anchors for the **Analytic Tradecraft and Source Integrity** lane include [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2026e]; [Agency, 2009]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **structured analytic judgment**. Learners use a **competing-hypotheses evidence table** and keep this boundary visible: No overclaiming, unsupported attribution, or bypass of reviewer challenge.

Frame. The classroom question centers on **CIA Tradecraft Primer: SATs for Intelligence Analysis**. Excluded actions stay explicit, and the **Structured-Judgment Lens** planning question is: Which assumptions, alternatives, confidence statements, and source limits must stay visible for review?

Inputs. For the **CIA Tradecraft Primer: SATs for Intelligence Analysis** scenario, use synthetic shipment notes, public policy excerpts, and a short instructor-provided event timeline. The Structured-Judgment Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **CIA Tradecraft Primer: SATs for Intelligence Analysis**, students write hypotheses, list evidence for and against each, mark assumptions, and assign confidence only after alternatives are tested. Pause whenever an inference about CIA Tradecraft Primer: SATs for Intelligence Analysis appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **CIA Tradecraft Primer: SATs for Intelligence Analysis** classroom scenario; unit artifact = competing-hypotheses evidence table; evidence = allowed inputs; method = structured reasoning and source-integrity review; output = an analytic note with a hypothesis table, confidence statement, dissent field, and collection gap list; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **CIA Tradecraft Primer: SATs for Intelligence Analysis** as "Structured-Judgment Lens confirms it" is not enough. The revision ties the claim to structured reasoning and source-integrity review, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **CIA Tradecraft Primer: SATs for Intelligence Analysis** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

57.2.4 Structured Analytic Techniques (SATs) practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Structured-Judgment Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**.

Triangulation anchors. In module 41's practice-sequence section, directly verified anchors for the **Analytic Tradecraft and Source Integrity** lane include [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2026e]; [Agency, 2009]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare CIA Tradecraft Primer: SATs for Intelligence Analysis, ICD 203 Analytic Standards: The Nine Tradecraft Standards, Psychology of Intelligence Analysis; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Analytic Tradecraft and Source Integrity** lane.
2. Frame	Answer the lens question: Which assumptions, alternatives, confidence statements, and source limits must stay visible for review?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for CIA Tradecraft Primer: SATs for Intelligence Analysis: analytic note with hypotheses, evidence table, confidence, and dissent fields.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the competing-hypotheses evidence table fields for CIA Tradecraft Primer: SATs for Intelligence Analysis.	Unit profile note.	Evidence artifacts include hypothesis table, assumption register.
4. Challenge	Test the misconception that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.	Failure-mode note.	The artifact applies the key distinction: separate reporting from inference, and inference from judgment.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

57.2.4.1 Structured Analytic Techniques (SATs) instructor notes: source reasoning, review points, and studio focus Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**. [237, 2026]; [266, 2026].

57.2.4.2 Structured Analytic Techniques (SATs) extension exercise: peer validation and refresh trigger review **Evidence anchor.** Section 57; [237, 2026].

Have learners swap artifacts and apply the **Structured-Judgment Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**.

57.2.5 Structured Analytic Techniques (SATs) knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 57; [237, 2026].

1. Explain how **CIA Tradecraft Primer: SATs for Intelligence Analysis** is defined here; name the source descriptor that supports the definition.
2. Contrast **CIA Tradecraft Primer: SATs for Intelligence Analysis** with **ICD 203 Analytic Standards: The Nine Tradecraft Standards** using the **Structured-Judgment Lens** artifact fields.
3. Identify one failure mode from the **Analytic Tradecraft and Source Integrity** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which assumption would change the judgment if it were false?
5. Correct this misconception: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

57.2.5.1 Structured Analytic Techniques (SATs) answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **CIA Tradecraft Primer: SATs for Intelligence Analysis** without source evidence, uncertainty, or a safe transfer task.

57.3 Structured Analytic Techniques (SATs) assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 57; [237, 2026].

57.3.1 Structured Analytic Techniques (SATs) evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 57; [237, 2026].

57.3.2 Structured Analytic Techniques (SATs) transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 57; [237, 2026].

57.3.2.1 Structured Analytic Techniques (SATs) lineage and source tradition: profile, concepts, and first anchors This sits in the **Analytic Tradecraft and Source Integrity** lineage: turning uncertainty into reviewable judgment through sourcing, alternatives, separated likelihood and confidence language, warning indicators, and explicit analytic lineage. [237, 2026]; [266, 2026].

57.3.2.2 Structured Analytic Techniques (SATs) working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 57; [237, 2026].
The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**, with provenance and reviewability throughout.

57.3.2.3 Structured Analytic Techniques (SATs) knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** reporting, assumptions, alternatives, confidence language, dissent, and source descriptors. [237, 2026]; [266, 2026].
- **Transforms:** hypothesis generation, evidence sorting, assumption challenge, confidence calibration, and dissent capture.
- **Outputs:** analytic note, hypothesis table, assumption list, and confidence statement.
- **Failure modes:** single-hypothesis reasoning, source laundering, confidence inflation, and suppressed dissent.

57.3.2.4 Structured Analytic Techniques (SATs) transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 57; [237, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**.
- **Evidence contract:** keep the **Analytic Tradecraft and Source Integrity** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as analytic note, hypothesis table, assumption list, and confidence statement that another reviewer can audit.

57.3.2.5 Structured Analytic Techniques (SATs) profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 57; [237, 2026].
The matched profile emphasizes turning uncertainty into reviewable judgment through sourcing, alternatives, separated likelihood and confidence language, warning indicators, and explicit analytic lineage. The method stack is key assumptions check, analysis of competing hypotheses, diagnosticity review, indicators and warnings, probability calibration, red-team review, collective tradecraft rating, and source descriptor audit; the local topic cluster is **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**.

57.3.3 Structured Analytic Techniques (SATs) evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 57; [237, 2026].
Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Analytic Tradecraft and Source Integrity** profile tells reviewers what evidence is strong enough for the module artifact built around **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**.

57.3.3.1 Structured Analytic Techniques (SATs) guide source spine: inherited keys and local citation roles Primary guide citations: [237, 2026]; [266, 2026]; [269, 2026]; [273, 2026]; [274, 2026]; [275, 2026]; [286, 2026]; [287, 2026]; [292, 2026]; [189, 2026]; [108, 2026]; [002, 2026]; [190, 2026]; [180, 2026]; [191, 2026]; [192, 2026]; [193, 2026]; [194, 2026]; [195, 2026]; [196, 2026]; [188, 2026]; [297, 2026]; [298, 2026]; [300, 2026]; [304, 2026]; [306, 2026]; [309, 2026]; [310, 2026].

57.3.3.2 Structured Analytic Techniques (SATs) verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [237, 2026]; [266, 2026].

Tier	What counts	How it is used
Source guide	[237, 2026]; [266, 2026]; [269, 2026]; [273, 2026]; [274, 2026]; [275, 2026]; [286, 2026]; [287, 2026]; [292, 2026]; [189, 2026]; [108, 2026]; [002, 2026]; [190, 2026]; [180, 2026]; [191, 2026]; [192, 2026]; [193, 2026]; [194, 2026]; [195, 2026]; [196, 2026]; [188, 2026]; [297, 2026]; [298, 2026]; [300, 2026]; [304, 2026]; [306, 2026]; [309, 2026]; [310, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 41's source-canon section, directly verified anchors for the **Analytic Tradecraft and Source Integrity** lane include [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2026e]; [Agency, 2009]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Maintenance rule: Perplexity may suggest candidates for **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards** and [237, 2026]; [266, 2026], but only directly verified source URLs are encoded as citations.

57.3.3.3 Structured Analytic Techniques (SATs) intelligence practice lens: evidence artifact and safety check Practice lens: **Structured-Judgment Lens** for **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**. [237, 2026]; [266, 2026].

Planning question: Which assumptions, alternatives, confidence statements, and source limits must stay visible for review?

Evidence artifact: analytic note with hypotheses, evidence table, confidence, and dissent fields.

Validation rule: separate raw reporting, inference, judgment, and recommendation before synthesis. Applied to **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**.

Handoff contract: handoff preserves alternatives, uncertainty, caveats, and revision history for downstream modules.

Safety check: avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence.

57.3.3.4 Structured Analytic Techniques (SATs) runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 57; [237, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	41.99	41.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Structured Analytic Techniques (SATs) to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Bounded autonomy, procurement, incident-response, and assurance studio	41.101	41.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Structured Analytic Techniques (SATs)	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Model-card, recoverability, retention, and learner-support evidence package	41.102	41.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Structured Analytic Techniques (SATs)	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
CIA Tradecraft Primer: SATs for Intelligence Analysis	41.1	41.1 CIA Tradecraft Primer: SATs for Intelligence Analysis	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
ICD 203 Analytic Standards: The Nine Tradecraft Standards	41.2	41.2 ICD 203 Analytic Standards: The Nine Tradecraft Standards	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Psychology of Intelligence Analysis (Heuer, CIA 1999)	41.3	41.3 Psychology of Intelligence Analysis (Heuer, CIA 1999)	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Structured Analytic Techniques (Heuer & Pherson, 2011)	41.4	41.4 Structured Analytic Techniques (Heuer & Pherson, 2011)	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Analysis of Competing Hypotheses (ACH)	41.4.1	41.4.1 Analysis of Competing Hypotheses (ACH)	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Devil's Advocacy and Red Teaming	41.4.2	41.4.2 Devil's Advocacy and Red Teaming	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Alternative Futures Analysis	41.4.3	41.4.3 Alternative Futures Analysis	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Brainstorming and Divergent Thinking Techniques	41.4.4	41.4.4 Brainstorming and Divergent Thinking Techniques	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Deception Detection SATs	41.4.5	41.4.5 Deception Detection SATs	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Key Assumptions Check	41.4.6	41.4.6 Key Assumptions Check	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Indicators Validator	41.4.7	41.4.7 Indicators Validator	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
What If? / Pre-Mortem Analysis	41.4.8	41.4.8 What If? / Pre-Mortem Analysis	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Analytic Tradecraft and the Intelligence Community (Tandfonline, 2014)	41.5	41.5 Analytic Tradecraft and the Intelligence Community (Tandfonline, 2014)	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Analytic Tradecraft Standards in Army Intelligence	41.6	41.6 Analytic Tradecraft Standards in Army Intelligence	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Cognitive Biases: Confirmation Bias, Anchoring, Groupthink in Intelligence	41.7	41.7 Cognitive Biases: Confirmation Bias, Anchoring, Groupthink in Intelligence	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
From Spycraft to Self-Mastery: SATs for Everyday Decision-Making	41.8	41.8 From Spycraft to Self-Mastery: SATs for Everyday Decision-Making	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence

57.3.3.5 Structured Analytic Techniques (SATs) reusable subsection contract: topic rows, artifacts, and safety duties Evidence anchor. Section 57; [237, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
CIA Tradecraft Primer: SATs for Intelligence Analysis	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
ICD 203 Analytic Standards: The Nine Tradecraft Standards	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Psychology of Intelligence Analysis (Heuer, CIA 1999)	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Structured Analytic Techniques (Heuer & Pherson, 2011)	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Analysis of Competing Hypotheses (ACH)	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Devil's Advocacy and Red Teaming	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Alternative Futures Analysis	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Brainstorming and Divergent Thinking Techniques	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Deception Detection SATs	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Key Assumptions Check	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Indicators Validator	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
What If? / Pre-Mortem Analysis	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Analytic Tradecraft and the Intelligence Community (Tandfonline, 2014)	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Analytic Tradecraft Standards in Army Intelligence	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Cognitive Biases: Confirmation Bias, Anchoring, Groupthink in Intelligence	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
From Spycraft to Self-Mastery: SATs for Everyday Decision-Making	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence

57.3.3.6 Structured Analytic Techniques (SATs) annotated source ledger: real titles and local contribution Each source cited by this **Analytic Tradecraft and Source Integrity** module is paired below with its real title and a one-line note on what it contributes to **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**.

Source	Cited work	What it contributes	Status
[237, 2026]	Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities	Official GAO AI accountability framework.	original source-guide
[266, 2026]	PROV Overview	A W3C Working Group Note from 2013 that provides an overview and roadmap for the PROV family of specifications for representing and exchanging provenance information on the web. It defines provenance as information about the entities, activities, and people involved in producing data, used to assess quality, reliability, and trustworthiness.	verified source-guide

Source	Cited work	What it contributes	Status
[269, 2026]	Data on the Web Best Practices	A W3C Recommendation, "Data on the Web Best Practices," published January 31, 2017 by the Data on the Web Best Practices Working Group. It offers 35 best practices for publishing and consuming data on the Web, covering metadata, licensing and provenance, data quality, dataset versioning, persistent URIs, machine-readable formats, vocabulary reuse, access methods, preservation, and feedback.	verified source-guide
[273, 2026]	WCAG 2 Overview	The W3C Web Accessibility Initiative overview of the Web Content Accessibility Guidelines (WCAG), an international standard for making web content accessible to people with disabilities. It explains that WCAG is organized around four principles (perceivable, operable, understandable, robust) with testable success criteria at three conformance levels (A, AA, AAA), and covers versions 2.0, 2.1, and 2.2.	verified source-guide
[274, 2026]	CAST Universal Design for Learning Guidelines version 3.0	The official CAST website for the Universal Design for Learning (UDL) Guidelines version 3.0, released in 2024. The framework offers research-based guidance for designing inclusive learning environments and is organized around three principles: Engagement (motivation and emotional support), Representation (accessible presentation of information), and Action and Expression (diverse means of participation and communication).	verified source-guide
[275, 2026]	Fact Sheet: New Rule on the Accessibility of Web Content and Mobile Apps Provided by State and Local Governments	A US Department of Justice fact sheet explaining the 2024 ADA Title II rule requiring state and local governments to make their web content and mobile apps accessible. It establishes WCAG 2.1 Level AA as the technical standard, applies to entities such as schools, courts, libraries, and transit agencies, and sets compliance deadlines of April 2027 for larger jurisdictions and April 2028 for smaller ones.	verified source-guide
[286, 2026]	Model Cards for Model Reporting	The arXiv abstract for "Model Cards for Model Reporting" (2018) by Mitchell, Wu, Zaldivar, and colleagues, which introduces a framework for transparent documentation of machine learning models. Model cards are short accompanying documents that report a model's benchmarked performance across varied conditions, including different cultural, demographic, and phenotypic groups, along with intended use, evaluation methodology, and deployment considerations.	verified source-guide

Source	Cited work	What it contributes	Status
[287, 2026]	Datasheets for Datasets	A 2018 arXiv paper proposing 'datasheets for datasets,' a standardized documentation framework for machine learning datasets modeled on electronic component datasheets. The authors argue the field lacks consistent dataset documentation, which creates risk in high-stakes applications, and propose that datasets be accompanied by documentation covering motivation, composition, collection process, recommended uses, and test results.	verified source-guide
[292, 2026]	Assessing Risks and Impacts of AI (ARIA): Pilot Evaluation Report	The ARIA 0.1 pilot evaluation report documents NIST's methodology for systematically assessing AI applications for risks and societal impacts, using a multi-layered evaluation approach across five participating organizations and seven submitted AI applications. The pilot employed three evaluation scenarios and three testing levels: model testing, red teaming, and field testing, supplemented by dialogue annotation, tester questionnaires, and structured measurement trees.	verified source-guide
[189, 2026]	A Tradecraft Primer - CSI	This primer will assist analysts in dealing with the perennial problems of intelligence.	original source-guide
[108, 2026]	Critical Thinking techniques	A Tradecraft Primer: Structured Analytic Techniques for Improving. Intelligence Analysis.	original source-guide
[002, 2026]	Objectivity	ICD 203 directs the heads of IC elements to designate a similar individual or office to respond.	original source-guide
[190, 2026]	Objectivity - Intelligence.gov	A page on Intelligence.gov, the U.S. Intelligence Community's public site, presenting objectivity as a core IC value. It explains that intelligence analysis must be performed and conveyed without distortion from personal or political bias, and references the standards codified in Intelligence Community Directive (ICD) 203 on analytic standards.	verified source-guide
[180, 2026]	Why Psychology of Intelligence Analysis Still Matters?	A SpecialEurasia article (2024) reviewing Richards J. Heuer Jr.'s 1999 work Psychology of Intelligence Analysis and arguing for its continued relevance. It summarizes Heuer's account of how cognitive biases such as confirmation bias, anchoring, and availability heuristics distort analytic judgment, and how analysts' backgrounds shape interpretation.	verified source-guide context; do not use as primary analytic support
[191, 2026]	Richards Heuer	A Wikipedia biography of Richards J. Heuer Jr. (1927-2018), a long-serving CIA intelligence analyst known for foundational contributions to analytic tradecraft. It describes his development of the Analysis of Competing Hypotheses method, his book 'Psychology of Intelligence Analysis' arguing that structured tools help analysts cope with cognitive bias and uncertainty, and his co-authored guide to Structured Analytic Techniques.	verified source-guide context; do not use as primary analytic support

Source	Cited work	What it contributes	Status
[192, 2026]	The Psychology of Intelligence Analysis	Psychology of Intelligence Analysis by Richards J. Heuer Jr., published by the Center for the Study of Intelligence, Central Intelligence Agency (1999). This foundational text examines the cognitive processes and mental limitations that affect intelligence analysts, focusing on how perception, memory, and bias shape judgment. It presents structured analytic methods intended to help analysts recognize and counteract these limitations and improve the quality of their reasoning.	verified source-guide context; do not use as primary analytic support
[193, 2026]	Structured Analytical Techniques - Organization of American States	Heuer provides a number of starter questions in his book.	original source-guide context; do not use as primary analytic support
[194, 2026]	Structured Analytic Techniques for Intelligence Analysis	A copy of "Structured Analytic Techniques for Intelligence Analysis" hosted on Scribd, a roughly 310-page professional reference on analytical methodologies for intelligence work. It presents systematic frameworks that analysts can use to process information, test hypotheses, identify patterns, and reach evidence-based conclusions while reducing bias. The document is oriented toward practitioners seeking to strengthen analytic rigor.	verified source-guide context; do not use as primary analytic support
[195, 2026]	Full article: Analytic Tradecraft and the Intelligence Community	The emphasis and visibility afforded analytic tradecraft in the Intelligence Community's analytic.	original source-guide context; do not use as primary analytic support
[196, 2026]	Analytic Tradecraft Standards - Army University Press	The nine analytic tradecraft standards in Intelligence Community Directive (ICD) 203, Analytic.	original source-guide context; do not use as primary analytic support
[188, 2026]	From Spycraft to Self-Mastery: How Structured Analytic Techniques	An article on Spotter Up by Eugene Nielsen arguing that structured analytic techniques (SATs) developed for intelligence analysis can improve everyday decision-making. It describes cognitive biases such as confirmation bias and overconfidence, then outlines categories of SATs including diagnostic, contrarian, imaginative, structuring, and decision-support methods.	verified source-guide context; do not use as primary analytic support
[297, 2026]	Intelligence Community Directive 203: Analytic Standards	Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products.	original source-guide
[298, 2026]	Intelligence Community Directives	Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations.	original source-guide
[300, 2026]	MITRE ATLAS	MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy.	original source-guide

Source	Cited work	What it contributes	Status
[304, 2026]	Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities	NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences.	verified source-guide
[306, 2026]	Artificial Intelligence	Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support.	original source-guide
[309, 2026]	STIX Version 2.1	An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection.	verified source-guide
[310, 2026]	TAXII Version 2.1	The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe).	verified source-guide

Where this sits. This module's overview is Section 57; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

57.3.4 Structured Analytic Techniques (SATs) governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 57; [237, 2026].

57.3.5 Structured Analytic Techniques (SATs) analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 41's governance-boundary section, directly verified anchors for the **Analytic Tradecraft and Source Integrity** lane include [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2026e]; [Agency, 2009]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **Analytic Tradecraft and Source Integrity** for **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**. [237, 2026]; [266, 2026].

Curriculum topic spine: CIA Tradecraft Primer: SATs for Intelligence Analysis, **ICD 203 Analytic Standards: The Nine Tradecraft Standards**, **Psychology of Intelligence Analysis (Heuer, CIA 1999)**. **Verified anchor cluster:** [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2026e]; [Agency, 2009]; [for the Study of Intelligence, 2002]; [for the Study of Intelligence, 1994]; [Agency, 2016].

Conceptual depth: turning uncertainty into reviewable judgment through sourcing, alternatives, separated likelihood and confidence language, warning indicators, and explicit analytic lineage.

Method stack: key assumptions check, analysis of competing hypotheses, diagnosticity review, indicators and warnings, probability calibration, red-team review, collective tradecraft rating, and source descriptor audit.

Composability contract: every agent output must preserve evidence, assumptions, judgments, likelihood, confidence, dissent, empirical limits, and change history as separable fields.

Known failure modes: source laundering, automation bias, hidden assumptions, collapsed likelihood/confidence language, hindsight certainty, SAT-as-bias-cure overclaiming, and visually persuasive but weakly sourced claims.

Defensive boundary: analysis remains educational and decision-supportive; it does not become tasking, targeting, covert collection, or policy advocacy. Applied to **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**.

Anchor	Why it matters here
[of the Director of National Intelligence, 2015]	Official ODNI analytic tradecraft standards directive. Checked as of 2026-05-21; role: source_quality_anchor.
[of the Director of National Intelligence, 2026d]	Official sourcing directive for traceability, citations, source descriptors, and source summaries. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026e]	Official ODNI explanation of analytic objectivity, ombuds, and tradecraft standards. Checked as of 2026-05-21; role: curriculum_anchor.
[Agency, 2009]	Official structured analytic techniques primer for bias checks, alternatives, and warning analysis. Checked as of 2026-05-21; role: curriculum_anchor.
[for the Study of Intelligence, 2002]	Official CIA Center for the Study of Intelligence essay on Kent's professionalization of intelligence analysis and analytic standards. Checked as of 2026-06-11; role: curriculum_anchor.
[for the Study of Intelligence, 1994]	Official CIA CSI republication of Kent's final essay on analyst-policy relations, warning, intention, and communication boundaries. Checked as of 2026-06-11; role: curriculum_anchor.
[Agency, 2016]	Defense intelligence structured-analysis primer for classroom analytic exercises. Checked as of 2026-05-21; role: curriculum_anchor.

57.3.5.1 Structured Analytic Techniques (SATs) evidence standard and citation floor: source families and discovery limits Official guidance supplies governance, safety, and legal constraints for the **Analytic Tradecraft and Source Integrity** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [237, 2026]; [266, 2026].

57.3.6 Structured Analytic Techniques (SATs) agentic boundary: assist, approve, block, and record

Evidence anchor. Section 57; [237, 2026].

AGEINT translation is bounded by the **Analytic Tradecraft and Source Integrity** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**.

57.3.6.1 Structured Analytic Techniques (SATs) permitted defensive utility: curriculum uses and safe outputs **Evidence anchor.** Section 57; [237, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**.

57.3.6.2 Structured Analytic Techniques (SATs) excluded operational boundary: blocked actions and stop rules Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [237, 2026]; [266, 2026] and **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

57.3.7 Structured Analytic Techniques (SATs) governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 57; [237, 2026].

Governance is practiced as a gate on the **Analytic Tradecraft and Source Integrity** lane. Learners use the **Structured-Judgment Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**.

57.3.7.1 Structured Analytic Techniques (SATs) governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [237, 2026]; [266, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Analytic Tradecraft and Source Integrity** failure modes and the **Structured-Judgment Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

57.3.7.2 Structured Analytic Techniques (SATs) evidence package handoff: appendices, records, and reuse **Evidence anchor.** Section 57; [237, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Structured-Judgment Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**.

57.3.7.3 Structured Analytic Techniques (SATs) current-source assurance: verified anchors and local artifact fit The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**. [237, 2026]; [266, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_odni_icd_203` for **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**?	Intelligence Community Directive 203: Analytic Standards; lane `source_quality_spine`; checked 2026-05-21.	analytic note with hypotheses, evidence table, confidence, and dissent fields; Official ODNI analytic tradecraft standards directive.
What does the module inherit from `official_odni_icd_206` for **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**?	Intelligence Community Directive 206: Sourcing Requirements for Disseminated Analytic Products; lane `analytic_tradecraft`; checked 2026-05-21.	analytic note with hypotheses, evidence table, confidence, and dissent fields; Official sourcing directive for traceability, citations, source descriptors, and source summaries.
What does the module inherit from `official_odni_objectivity` for **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**?	Objectivity and IC Analytic Standards; lane `analytic_tradecraft`; checked 2026-05-21.	analytic note with hypotheses, evidence table, confidence, and dissent fields; Official ODNI explanation of analytic objectivity, ombuds, and tradecraft standards.
What does the module inherit from `official_cia_tradecraft_primer` for **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**?	A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis; lane `analytic_tradecraft`; checked 2026-05-21.	analytic note with hypotheses, evidence table, confidence, and dissent fields; Official structured analytic techniques primer for bias checks, alternatives, and warning analysis.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 57; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

57.3.8 Structured Analytic Techniques (SATs) assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 57; [237, 2026].

57.3.9 Structured Analytic Techniques (SATs) assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 57; [237, 2026].

57.3.9.1 Structured Analytic Techniques (SATs) capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**.
Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards** and [237, 2026]; [266, 2026].

57.3.9.2 Structured Analytic Techniques (SATs) instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards** and [237, 2026]; [266, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

57.3.9.3 Structured Analytic Techniques (SATs) assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
CIA Tradecraft Primer: SATs for Intelligence Analysis	Completed **analytic note with hypotheses, evidence table, confidence, and dissent fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
ICD 203 Analytic Standards: The Nine Tradecraft Standards	Completed **analytic note with hypotheses, evidence table, confidence, and dissent fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Psychology of Intelligence Analysis (Heuer, CIA 1999)	Completed **analytic note with hypotheses, evidence table, confidence, and dissent fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

57.3.10 Structured Analytic Techniques (SATs) refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [237, 2026]; [266, 2026] and **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**.

57.3.10.1 Structured Analytic Techniques (SATs) refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**. The local signals begin with [237, 2026]; [266, 2026].

57.3.10.2 Structured Analytic Techniques (SATs) claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**, and the source spine for these checks begins with [237, 2026]; [266, 2026].

57.3.11 Structured Analytic Techniques (SATs) reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [237, 2026]; [266, 2026].
Triangulation anchors. In module 41's review-checklist section, directly verified anchors for the **Analytic Tradecraft and Source Integrity** lane include [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2026e]; [Agency, 2009]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards**. [237, 2026]; [266, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

57.3.12 Structured Analytic Techniques (SATs) learning-path links: module map, overview, and curriculum atlas

Follow the cross-links to move between **CIA Tradecraft Primer: SATs for Intelligence Analysis; ICD 203 Analytic Standards: The Nine Tradecraft Standards** and the rest of the curriculum without losing the source spine: orientation first, then the parent unit, then the modules on either side. Primary sources: [237, 2026]; [266, 2026].

Section 2, Section 56, Section 58

58 Advanced Analysis Methods

58.0.1 Advanced Analysis Methods figures and course links: visual evidence, source flow, and navigation

The module uses Figure 125, Figure 126, Figure 127, Figure 128, and Figure 116 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.

Navigation links: Section 2, Section 56, Section 57, Section 59.

This module teaches the **Analytic Tradecraft and Source Integrity** lane through a bounded, source-backed coursebook chapter. [237, 2026]; [266, 2026].

58.1 Analytic Tradecraft and Source Integrity frame for Advanced Analysis Methods: source context, topic focus, and reader task

Evidence anchor. Section 58; [237, 2026].

58.1.1 Advanced Analysis Methods orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 58; [237, 2026].

58.1.2 Advanced Analysis Methods conceptual primer: source context, core model, and reader task

This chapter teaches analytic tradecraft as disciplined judgment under uncertainty: claims become useful only when evidence, assumptions, alternatives, confidence, and dissent remain visible. The chapter uses **Structured-Judgment Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**.

The central distinction is to separate reporting from inference, and inference from judgment. Core topics include **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis; Timeline Analysis and Event Sequencing**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.

Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2026e]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [237, 2026]; [266, 2026].

Learners move from vocabulary and the **Structured-Judgment Lens** distinction through topic lessons on **Red Cell Analysis and Adversarial Wargaming** with evidence and misconception checks, then assemble an **analytic note with hypotheses, evidence table, confidence, and dissent fields** with safety and rights gates.

58.1.3 Advanced Analysis Methods learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 58; [237, 2026].

- Connect **Red Cell Analysis and Adversarial Wargaming and Network Analysis: Link Charts, Activity Matrices, Social Network Analysis** to **Analytic Tradecraft and Source Integrity** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build an **analytic note with hypotheses, evidence table, confidence, and dissent fields** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate reporting from inference, and inference from judgment; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as source laundering, automation bias, hidden assumptions, collapsed likelihood/confidence language, hindsight certainty, SAT-as-bias-cure overclaiming, and visually persuasive but weakly sourced claims, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: analysis remains educational and decision-supportive; it does not become tasking, targeting, covert collection, or policy advocacy.

58.1.4 Advanced Analysis Methods core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 58; [237, 2026].

Term	Working definition
Source descriptor	a compact statement of where evidence came from and what it can support
Assumption	a claim accepted for analysis that still needs challenge
Alternative hypothesis	a plausible explanation that competes with the favored account
Confidence	a calibrated expression of evidentiary strength and analytic uncertainty
Dissent	a documented disagreement that preserves minority reasoning for review
Red Cell Analysis and Adversarial Wargaming	Key terms: Red, Cell, Analysis.
Network Analysis: Link Charts, Activity…	Key terms: Network, Analysis, Link.

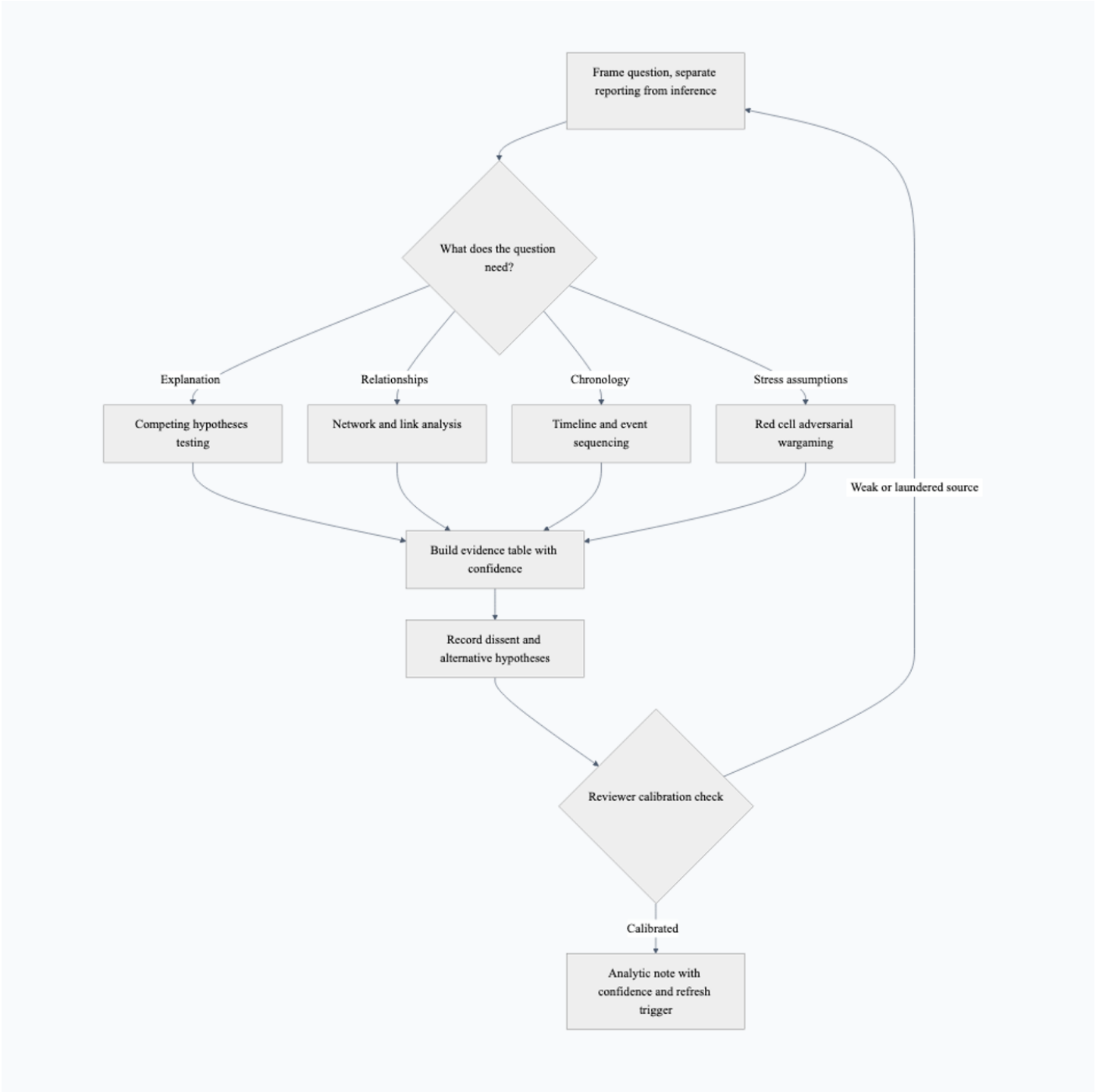


Figure 125: A decision tree that helps an analyst choose a structured method by the shape of the question while keeping evidence, confidence, and dissent visible. It is anchored to the epistemic rigor and analytic tradecraft / advanced analysis methods section; use it to inspect Frame question, separate reporting from inference, Competing hypotheses testing, Network and link analysis, and Timeline and event sequencing while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

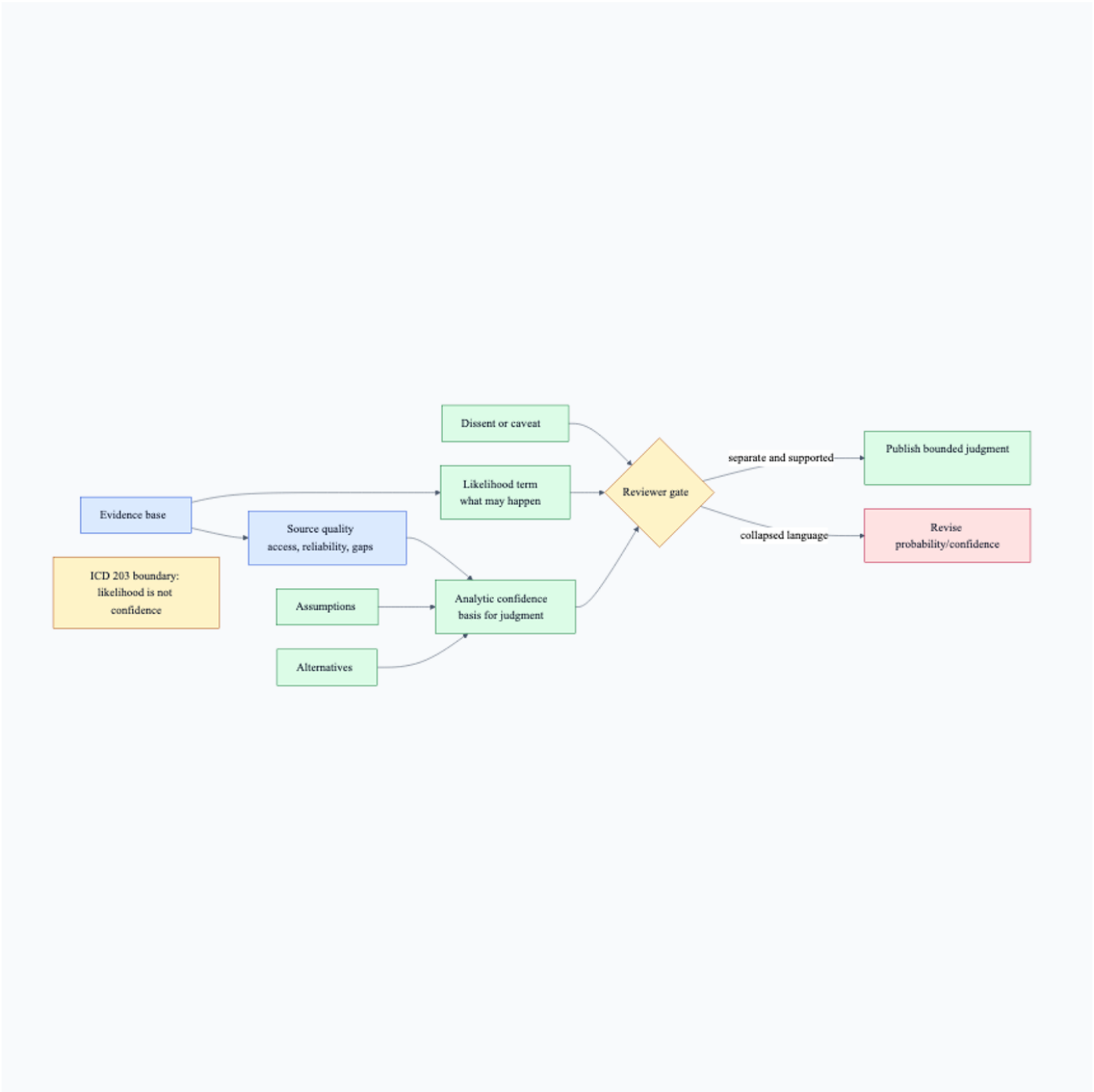


Figure 126: Source-backed conceptual schematic for ICD 203-style analytic statements: likelihood terms, confidence, source quality, assumptions, alternatives, and dissent are recorded as separate fields before release. It is anchored to the epistemic rigor and analytic tradecraft / advanced analysis methods section; use it to inspect Evidence base, Likelihood term what may happen, Source quality access, reliability, gaps, and Analytic confidence basis for judgment while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

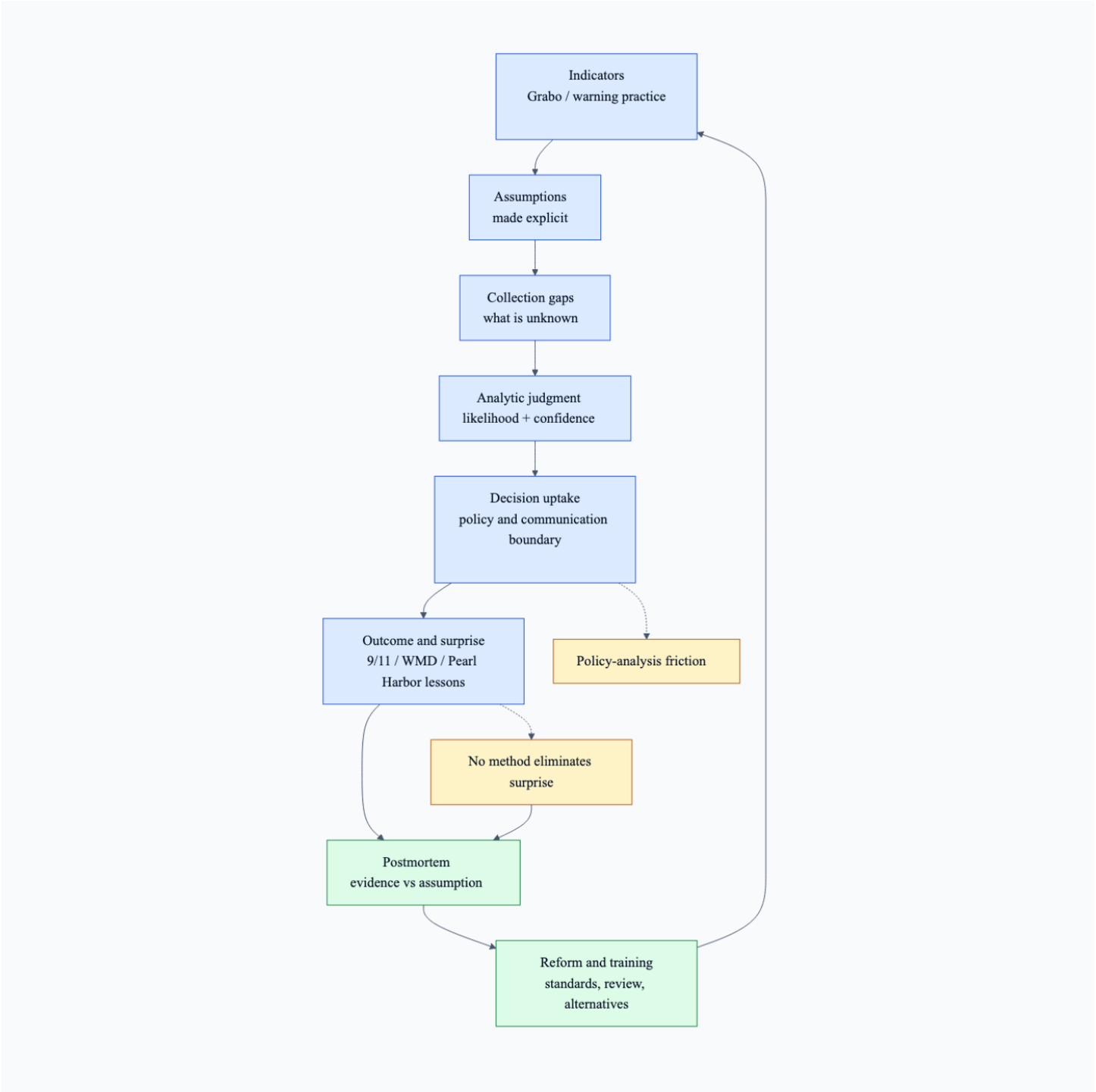


Figure 127: Source-backed conceptual schematic linking warning indicators, assumptions, collection gaps, decision uptake, postmortem findings, and reform learning without implying that any single technique can eliminate surprise. In the epistemic rigor and analytic tradecraft / advanced analysis methods section, it lets readers compare Indicators Grabo / warning practice, Assumptions made explicit, Collection gaps what is unknown, and Analytic judgment likelihood + confidence so the visual functions as a traceable course aid rather than an unscoped assertion.

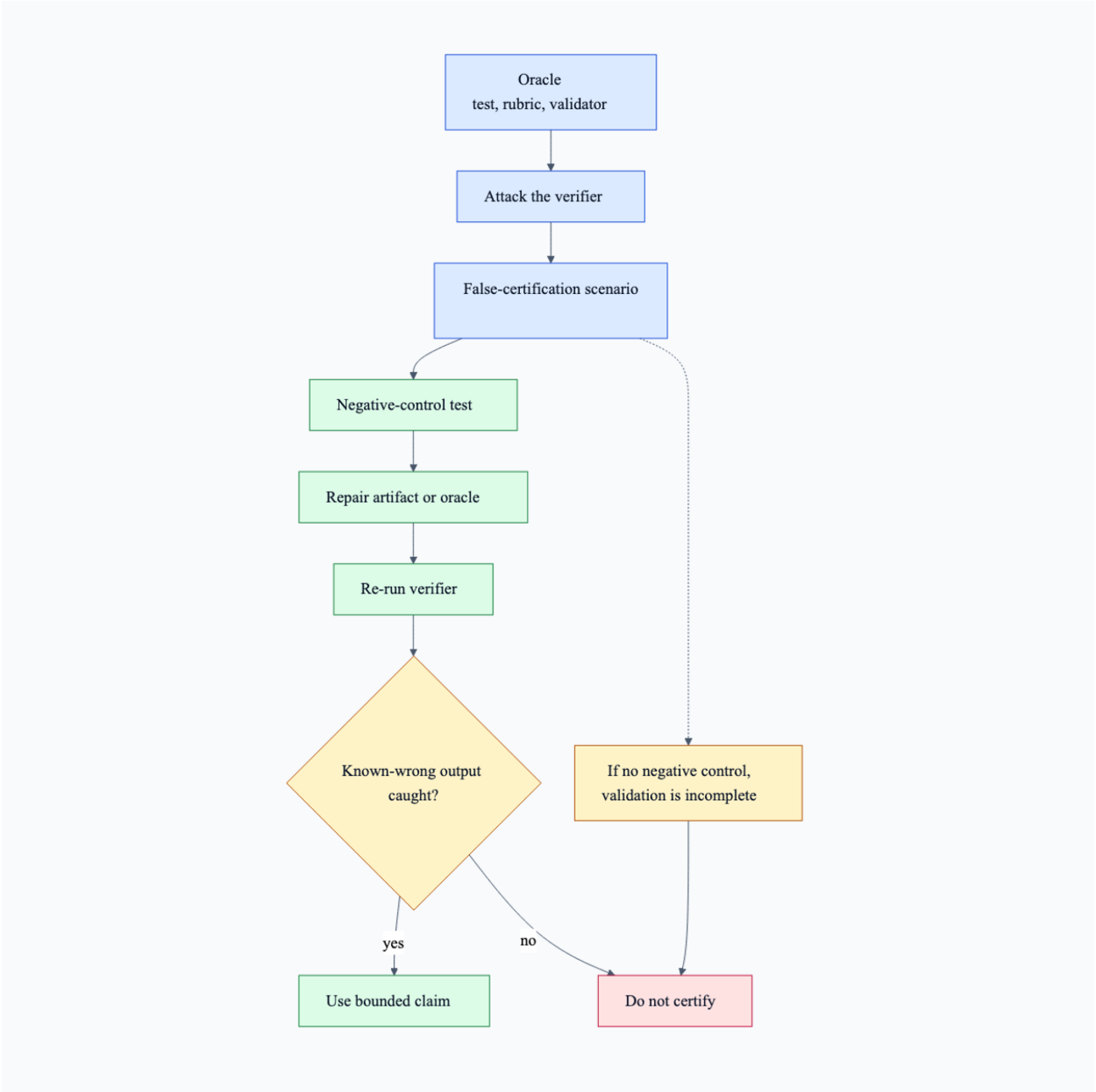


Figure 128: Source-backed conceptual schematic showing how AGEINT treats validators, rubrics, and rendered claims as attackable artifacts: a false-certification scenario creates a negative control before the claim is repaired and rechecked. In the epistemic rigor and analytic tradecraft / advanced analysis methods section, it lets readers compare Oracle test, rubric, validator, Attack the verifier, False-certification scenario, and Negative-control test so the visual functions as a traceable course aid rather than an unscoped assertion.

58.2 Structured-Judgment Lens path for Advanced Analysis Methods: lesson cluster, safe artifact, and review

Evidence anchor. Section 58; [237, 2026].

58.2.1 Advanced Analysis Methods practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 58; [237, 2026].

58.2.2 Advanced Analysis Methods topic lessons: source-backed concepts and transfer tasks

This module builds analytic tradecraft as disciplined judgment under uncertainty: claims become useful only when evidence, assumptions, alternatives, confidence, and dissent remain visible. The sequence opens with **Red Cell Analysis and Adversarial Wargaming**, **Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**, **Timeline Analysis and Event Sequencing** and applies the **Structured-Judgment Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 116; module overview Section 58; curriculum atlas Section 2.

Triangulation anchors. In module 42's topic-lessons section, directly verified anchors for the **Analytic Tradecraft and Source Integrity** lane include [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2026e]; [Agency, 2009]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

58.2.2.1 Lesson 1: Red Cell Analysis and Adversarial Wargaming **Concept. Red Cell Analysis and Adversarial Wargaming** uses red-cell review to surface disconfirming evidence and assumptions before dissemination.

Why it matters. Red Cell Analysis and Adversarial Wargaming connects classroom vocabulary to Analytic Tradecraft and Source Integrity practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Red Cell Analysis and Adversarial Wargaming rests on [300, 2026], [304, 2026], and [306, 2026]. The closest source to this row notes: NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Use them for fixing what **Red Cell Analysis and Adversarial Wargaming** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. Read **Red Cell Analysis and Adversarial Wargaming** against the works cited for this row. [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Red Cell Analysis**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must separate the source descriptor, the bounded judgment about **Red Cell Analysis and Adversarial**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape **Red Cell Analysis and Adversarial Wargaming** work as a **competing-hypotheses evidence table** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Red Cell Analysis and Adversarial Wargaming**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. Reuse the **Red Cell Analysis and Adversarial Wargaming** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

58.2.2.2 Lesson 2: Network Analysis: Link Charts, Activity Matrices, Social Network Analysis **Concept. Network Analysis: Link Charts, Activity Matrices, Social Network Analysis** — Build link charts from sample entities with provenance, confidence, and explicit gaps—not live targeting.

Why it matters. Without explicit treatment of **Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**, collapsing reporting, inference, and judgment into one line undermines structured reasoning and source-integrity review; the lesson builds the habit to separate reporting from inference, and inference from judgment.

Source support. Network Analysis: Link Charts, Activity Matrices, Social Network Analysis rests on [309, 2026], [310, 2026], and [300, 2026]. The closest source to this row notes: It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). Use them for fixing what **Network Analysis: Link Charts, Activity Matrices, Social Network Analysis** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. Read **Network Analysis: Link Charts, Activity Matrices, Social Network Analysis** against the works cited for this row. [309, 2026] An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection. [310, 2026] The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Network Analysis**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must separate the source descriptor, the bounded judgment about **Network Analysis**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape **Network Analysis: Link Charts, Activity Matrices, Social Network Analysis** work as a **competing-hypotheses evidence table** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. Reuse the **Network Analysis: Link Charts, Activity Matrices, Social Network Analysis** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

58.2.2.3 Lesson 3: Timeline Analysis and Event Sequencing **Concept. Timeline Analysis and Event Sequencing** — Sequence events with source timestamps, uncertainty bands, and alternative orderings before inferring causality.

Why it matters. Timeline Analysis and Event Sequencing connects classroom vocabulary to Analytic Tradecraft and Source Integrity practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Timeline Analysis and Event Sequencing rests on [297, 2026] and [298, 2026]. The most specific cited work observes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for pinning down the scope of **Timeline Analysis and Event Sequencing**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. Read **Timeline Analysis and Event Sequencing** against the works cited for this row. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. Build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must separate the source descriptor, the bounded judgment about **Timeline Analysis and Event Sequencing**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape this subject work as a **competing-hypotheses evidence table** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Timeline Analysis and Event Sequencing**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. Transfer **Timeline Analysis and Event Sequencing** from this module to a second motif by preserving structured reasoning and source-integrity review, replacing action with audit, and naming the blocked use.

58.2.2.4 Lesson 4: Collection Management: Requirements, Gaps, Tasking Concept. Collection Management: Requirements, Gaps, Tasking — Match intelligence requirements to least-intrusive source disciplines with explicit minimization and feedback to the customer.

Why it matters. Collection Management matters in the **Analytic Tradecraft and Source Integrity** lane because structured reasoning and source-integrity evidence must stay separate from judgment; collapsing reporting, inference, and judgment into one line is a common failure.

Source support. Collection Management: Requirements, Gaps, Tasking rests on [309, 2026], [310, 2026], and [300, 2026]. The most specific cited work observes: It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). Use them for fixing what **Collection Management: Requirements, Gaps, Tasking** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. Ground **Collection Management** in the evidence the row cites. [309, 2026] An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection. [310, 2026] The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Collection Management**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must separate the source descriptor, the bounded judgment about **Collection Management**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape **Collection Management** work as a **competing-hypotheses evidence table** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Collection Management**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. Transfer **Collection Management** from this module to a second motif by preserving structured reasoning and source-integrity review, replacing action with audit, and naming the blocked use.

58.2.2.5 Lesson 5: Writing Intelligence Products: Assessments, Estimates, Warnings Concept. Writing Intelligence Products: Assessments, Estimates, Warnings — Draft intelligence products with analytic line, caveats, audience, and dissemination marks.

Why it matters. Analysts use **Writing Intelligence Products** to separate reporting from inference, and inference from judgment. A defensible treatment names the judgment it enables for structured reasoning and source-integrity review, the proof limit that collapsing reporting, inference, and judgment into one line would otherwise hide, and the reviewer accountable for challenge.

Source support. Writing Intelligence Products: Assessments, Estimates, Warnings rests on [297, 2026] and [298, 2026]. The closest source to this row notes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for the working definition that **Writing Intelligence Products: Assessments, Estimates, Warnings** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. Ground **Writing Intelligence Products** in the evidence the row cites. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Writing Intelligence Products**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must separate the source descriptor, the bounded judgment about **Writing Intelligence Products**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape **Writing Intelligence Products** work as a **competing-hypotheses evidence table** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Writing Intelligence Products**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. Transfer **Writing Intelligence Products** from this module to a second motif by preserving structured reasoning and source-integrity review, replacing action with audit, and naming the blocked use.

58.2.2.6 Lesson 6: Communicating Uncertainty: Analytic Line vs. Raw Reporting Concept. Communicating Uncertainty: Analytic Line vs. Raw Reporting — Separate raw reporting from assessed analytic line with explicit confidence and dissent.

Why it matters. Communicating Uncertainty matters in the **Analytic Tradecraft and Source Integrity** lane because structured reasoning and source-integrity evidence must stay separate from judgment; collapsing reporting, inference, and judgment into one line is a common failure.

Source support. Communicating Uncertainty: Analytic Line vs. Raw Reporting rests on [297, 2026] and [298, 2026]. The most specific cited work observes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for the claim that **Communicating Uncertainty: Analytic Line vs. Raw Reporting** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. Ground **Communicating Uncertainty** in the evidence the row cites. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Communicating Uncertainty**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must separate the source descriptor, the bounded judgment about **Communicating Uncertainty**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape **Communicating Uncertainty** work as a **competing-hypotheses evidence table** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Communicating Uncertainty**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. Transfer **Communicating Uncertainty** from this module to a second motif by preserving structured reasoning and source-integrity review, replacing action with audit, and naming the blocked use.

58.2.2.7 Lesson 7: Machine-Assisted Analysis: When to Automate, When to Require Human Judgment

Concept. Machine-Assisted Analysis: When to Automate, When to Require Human Judgment — Decide automation boundaries with logging, evaluation, and mandatory human review gates.

Why it matters. Machine-Assisted Analysis connects classroom vocabulary to Analytic Tradecraft and Source Integrity practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Machine-Assisted Analysis: When to Automate, When to Require Human Judgment rests on [297, 2026] and [298, 2026]. The most specific cited work observes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for fixing what **Machine-Assisted Analysis: When to Automate, When to Require Human Judgment** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d].

Evidence to inspect. Read **Machine-Assisted Analysis** against the works cited for this row. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Machine-Assisted Analysis**, build a **analytic note with hypotheses, evidence table, confidence, and dissent fields** for this structured reasoning and source-integrity review topic. The artifact must separate the source descriptor, the bounded judgment about **Machine-Assisted Analysis**, the analytic caveat, the confidence note, the excluded-inference boundary, and the reviewer who logs dissent. Shape **Machine-Assisted Analysis** work as a **competing-hypotheses evidence table** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Machine-Assisted Analysis**: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

Transfer task. Reuse the **Machine-Assisted Analysis** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

58.2.3 Advanced Analysis Methods worked safe example: synthetic inputs, evidence, and review

Worked example: a synthetic analyst cell evaluates whether a benign supplier delay signals normal friction or elevated risk. [237, 2026]; [266, 2026].

Triangulation anchors. In module 42's worked-example section, directly verified anchors for the **Analytic Tradecraft and Source Integrity** lane include [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2026e]; [Agency, 2009]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **structured analytic judgment**. Learners use a **competing-hypotheses evidence table** and keep this boundary visible: No overclaiming, unsupported attribution, or bypass of reviewer challenge.

Frame. The classroom question centers on **Red Cell Analysis and Adversarial Wargaming**. Excluded actions stay explicit, and the **Structured-Judgment Lens** planning question is: Which assumptions, alternatives, confidence statements, and source limits must stay visible for review?

Inputs. For the **Red Cell Analysis and Adversarial Wargaming** scenario, use synthetic shipment notes, public policy excerpts, and a short instructor-provided event timeline. The Structured-Judgment Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Red Cell Analysis and Adversarial Wargaming**, students write hypotheses, list evidence for and against each, mark assumptions, and assign confidence only after alternatives are tested. Pause whenever an inference about Red Cell Analysis and Adversarial Wargaming appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Red Cell Analysis and Adversarial Wargaming** classroom scenario; unit artifact = competing-hypotheses evidence table; evidence = allowed inputs; method = structured reasoning and source-integrity review; output = an analytic note with a hypothesis table, confidence statement, dissent field, and collection gap list; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Red Cell Analysis and Adversarial Wargaming** as "Structured-Judgment Lens confirms it" is not enough. The revision ties the claim to structured reasoning and source-integrity review, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Red Cell Analysis and Adversarial Wargaming** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

58.2.4 Advanced Analysis Methods practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Structured-Judgment Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**.

Triangulation anchors. In module 42's practice-sequence section, directly verified anchors for the **Analytic Tradecraft and Source Integrity** lane include [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence,

2026e]; [Agency, 2009]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Red Cell Analysis and Adversarial Wargaming, Network Analysis: Link Charts, Activity Matrices, Social Network Analysis, Timeline Analysis and Event Sequencing; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Analytic Tradecraft and Source Integrity** lane.
2. Frame	Answer the lens question: Which assumptions, alternatives, confidence statements, and source limits must stay visible for review?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Red Cell Analysis and Adversarial Wargaming: analytic note with hypotheses, evidence table, confidence, and dissent fields.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the competing-hypotheses evidence table fields for Red Cell Analysis and Adversarial Wargaming.	Unit profile note.	Evidence artifacts include hypothesis table, assumption register.
4. Challenge	Test the misconception that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.	Failure-mode note.	The artifact applies the key distinction: separate reporting from inference, and inference from judgment.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

58.2.4.1 Advanced Analysis Methods instructor notes: source reasoning, review points, and studio focus Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**. [237, 2026]; [266, 2026].

58.2.4.2 Advanced Analysis Methods extension exercise: peer validation and refresh trigger review **Evidence anchor.** Section 58; [237, 2026].

Have learners swap artifacts and apply the **Structured-Judgment Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**.

58.2.5 Advanced Analysis Methods knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 58; [237, 2026].

1. Explain how **Red Cell Analysis and Adversarial Wargaming** is defined here; name the source descriptor that supports the definition.
2. Contrast **Red Cell Analysis and Adversarial Wargaming** with **Network Analysis: Link Charts, Activity Matrices, Social Network Analysis** using the **Structured-Judgment Lens** artifact fields.
3. Identify one failure mode from the **Analytic Tradecraft and Source Integrity** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which assumption would change the judgment if it were false?
5. Correct this misconception: that a confident narrative is the same as a tested, source-backed judgment with its alternatives and confidence stated.

58.2.5.1 Advanced Analysis Methods answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Red Cell Analysis and Adversarial Wargaming** without source evidence, uncertainty, or a safe transfer task.

58.3 Advanced Analysis Methods assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 58; [237, 2026].

58.3.1 Advanced Analysis Methods evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 58; [237, 2026].

58.3.2 Advanced Analysis Methods transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 58; [237, 2026].

58.3.2.1 Advanced Analysis Methods lineage and source tradition: profile, concepts, and first anchors This sits in the **Analytic Tradecraft and Source Integrity** lineage: turning uncertainty into reviewable judgment through sourcing, alternatives, separated likelihood and confidence language, warning indicators, and explicit analytic lineage. [237, 2026]; [266, 2026].

58.3.2.2 Advanced Analysis Methods working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 58; [237, 2026].
The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**, with provenance and reviewability throughout.

58.3.2.3 Advanced Analysis Methods knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** reporting, assumptions, alternatives, confidence language, dissent, and source descriptors. [237, 2026]; [266, 2026].
- **Transforms:** hypothesis generation, evidence sorting, assumption challenge, confidence calibration, and dissent capture.
- **Outputs:** analytic note, hypothesis table, assumption list, and confidence statement.
- **Failure modes:** single-hypothesis reasoning, source laundering, confidence inflation, and suppressed dissent.

58.3.2.4 Advanced Analysis Methods transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 58; [237, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**.
- **Evidence contract:** keep the **Analytic Tradecraft and Source Integrity** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as analytic note, hypothesis table, assumption list, and confidence statement that another reviewer can audit.

58.3.2.5 Advanced Analysis Methods profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 58; [237, 2026].
The matched profile emphasizes turning uncertainty into reviewable judgment through sourcing, alternatives, separated likelihood and confidence language, warning indicators, and explicit analytic lineage. The method stack is key assumptions check, analysis of competing hypotheses, diagnosticity review, indicators and warnings, probability calibration, red-team review, collective tradecraft rating, and source descriptor audit; the local topic cluster is **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**.

58.3.3 Advanced Analysis Methods evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 58; [237, 2026].
Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Analytic Tradecraft and Source Integrity** profile tells reviewers what evidence is strong enough for the module artifact built around **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**.

58.3.3.1 Advanced Analysis Methods guide source spine: inherited keys and local citation roles Primary guide citations: [237, 2026]; [266, 2026]; [270, 2026]; [276, 2026]; [277, 2026]; [284, 2026]; [288, 2026]; [289, 2026]; [293, 2026]; [297, 2026]; [298, 2026]; [300, 2026]; [304, 2026]; [306, 2026]; [309, 2026]; [310, 2026].

58.3.3.2 Advanced Analysis Methods verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [237, 2026]; [266, 2026].

Tier	What counts	How it is used
Source guide	[237, 2026]; [266, 2026]; [270, 2026]; [276, 2026]; [277, 2026]; [284, 2026]; [288, 2026]; [289, 2026]; [293, 2026]; [297, 2026]; [298, 2026]; [300, 2026]; [304, 2026]; [306, 2026]; [309, 2026]; [310, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 42's source-canon section, directly verified anchors for the **Analytic Tradecraft and Source Integrity** lane include [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2026e]; [Agency, 2009]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Maintenance rule: Perplexity may suggest candidates for **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis** and [237, 2026]; [266, 2026], but only directly verified source URLs are encoded as citations.

58.3.3.3 Advanced Analysis Methods intelligence practice lens: evidence artifact and safety check Practice lens: **Structured-Judgment Lens** for **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**. [237, 2026]; [266, 2026].

Planning question: Which assumptions, alternatives, confidence statements, and source limits must stay visible for review?

Evidence artifact: analytic note with hypotheses, evidence table, confidence, and dissent fields.

Validation rule: separate raw reporting, inference, judgment, and recommendation before synthesis. Applied to **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**.

Handoff contract: handoff preserves alternatives, uncertainty, caveats, and revision history for downstream modules.

Safety check: avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence.

58.3.3.4 Advanced Analysis Methods runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 58; [237, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	42.99	42.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Advanced Analysis Methods to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Bounded autonomy, procurement, incident-response, and assurance studio	42.101	42.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Advanced Analysis Methods	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Model-card, recoverability, retention, and learner-support evidence package	42.102	42.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Advanced Analysis Methods	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Red Cell Analysis and Adversarial Wargaming	42.1	42.1 Red Cell Analysis and Adversarial Wargaming	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Network Analysis: Link Charts, Activity Matrices, Social Network Analysis	42.2	42.2 Network Analysis: Link Charts, Activity Matrices, Social Network Analysis	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Timeline Analysis and Event Sequencing	42.3	42.3 Timeline Analysis and Event Sequencing	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Collection Management: Requirements, Gaps, Tasking	42.4	42.4 Collection Management: Requirements, Gaps, Tasking	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Writing Intelligence Products: Assessments, Estimates, Warnings	42.5	42.5 Writing Intelligence Products: Assessments, Estimates, Warnings	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Communicating Uncertainty: Analytic Line vs. Raw Reporting	42.6	42.6 Communicating Uncertainty: Analytic Line vs. Raw Reporting	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Machine-Assisted Analysis: When to Automate, When to Require Human Judgment	42.7	42.7 Machine-Assisted Analysis: When to Automate, When to Require Human Judgment	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence

58.3.3.5 Advanced Analysis Methods reusable subsection contract: topic rows, artifacts, and safety duties **Evidence anchor.** Section 58; [237, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Red Cell Analysis and Adversarial Wargaming	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Network Analysis: Link Charts, Activity Matrices, Social Network Analysis	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Timeline Analysis and Event Sequencing	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Collection Management: Requirements, Gaps, Tasking	Requirements-to-Evidence Lens	requirements matrix with source descriptors, caveats, and collection limits	exclude live collection, recruitment, surveillance, interception, tracking, and identity exposure
Writing Intelligence Products: Assessments, Estimates, Warnings	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Communicating Uncertainty: Analytic Line vs. Raw Reporting	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence
Machine-Assisted Analysis: When to Automate, When to Require Human Judgment	Structured-Judgment Lens	analytic note with hypotheses, evidence table, confidence, and dissent fields	avoid policy advocacy, certainty inflation, source laundering, and claims without traceable evidence

58.3.3.6 Advanced Analysis Methods annotated source ledger: real titles and local contribution Each source cited by this **Analytic Tradecraft and Source Integrity** module is paired below with its real title and a one-line note on what it contributes to **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**.

Source	Cited work	What it contributes	Status
[237, 2026]	Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities	Official GAO AI accountability framework.	original source-guide
[266, 2026]	PROV Overview	A W3C Working Group Note from 2013 that provides an overview and roadmap for the PROV family of specifications for representing and exchanging provenance information on the web. It defines provenance as information about the entities, activities, and people involved in producing data, used to assess quality, reliability, and trustworthiness.	verified source-guide

Source	Cited work	What it contributes	Status
[270, 2026]	NIST Big Data Interoperability Framework	NIST Special Publication 1500-1 (revised edition by Chang and Grady) establishes foundational terminology and consensus definitions for Big Data through the NIST Big Data Public Working Group. The volume defines Big Data characteristics, taxonomy, and a reference architecture assigning roles to Application Providers, Data Consumers, Data Providers, and System Orchestrators.	verified source-guide
[276, 2026]	What is a Data Protection Impact Assessment and When Is This Mandatory?	A European Data Protection Board FAQ page, part of its data protection guide for small businesses, explaining Data Protection Impact Assessments (DPIAs) and when they are mandatory. It describes a DPIA as a written assessment of the impact of a planned processing operation, required when processing poses high risks to individuals' rights.	verified source-guide
[277, 2026]	Endorsed WP29 Guidelines	This is a European Data Protection Board webpage listing guidelines and documents originating from the Article 29 Working Party that the EDPB endorsed at its first plenary meeting. The catalogued materials relate to the GDPR and cover topics such as consent and transparency, data breach notification, automated decision-making and profiling, data protection impact assessments, data protection officers, and binding corporate rules.	verified source-guide
[284, 2026]	Verifiable Credential Data Integrity 1.0	The W3C Recommendation for Verifiable Credential Data Integrity 1.0, published May 2025, defining mechanisms for ensuring the authenticity and integrity of verifiable credentials using cryptographic proofs. It specifies a process of data transformation, hashing, and proof generation, and a corresponding verification procedure, along with a proof data model containing properties such as type, verification method, purpose, and proof value.	verified source-guide
[288, 2026]	Algorithmic Transparency Recording Standard Hub	A GOV.UK collection page serving as the hub for the UK Algorithmic Transparency Recording Standard (ATRS), maintained by the Government Digital Service. It provides a standardized template for documenting public-sector use of algorithmic tools, completion guidance, policy on scope and compliance, and a searchable repository of published transparency records.	verified source-guide
[289, 2026]	Guidance for Organisations Using the Algorithmic Transparency Recording Standard	This is a GOV.UK guidance page published by the Government Digital Service that instructs public sector organizations on completing the Algorithmic Transparency Recording Standard (ATRS) template and publishing their records to the GOV.UK repository. It applies both to central government bodies required to publish under mandatory policy and to other public sector bodies doing so voluntarily.	verified source-guide

Source	Cited work	What it contributes	Status
[293, 2026]	Inventory of NARA Artificial Intelligence (AI) Use Cases	The National Archives and Records Administration (NARA) official inventory of its artificial intelligence use cases, documenting 14 projects across deployed, pilot, and planned stages. Deployed efforts include workplace productivity tools, automated tagging for museum experiences, and historical record retrieval, while pilots cover PII detection and redaction, semantic search, and metadata generation, and planned work targets FOIA processing and public search.	verified source-guide
[297, 2026]	Intelligence Community Directive 203: Analytic Standards	Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products.	original source-guide
[298, 2026]	Intelligence Community Directives	Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations.	original source-guide
[300, 2026]	MITRE ATLAS	MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy.	original source-guide
[304, 2026]	Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities	NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences.	verified source-guide
[306, 2026]	Artificial Intelligence	Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support.	original source-guide
[309, 2026]	STIX Version 2.1	An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection.	verified source-guide
[310, 2026]	TAXII Version 2.1	The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe).	verified source-guide

Where this sits. This module's overview is Section 58; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

58.3.4 Advanced Analysis Methods governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 58; [237, 2026].

58.3.5 Advanced Analysis Methods analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 42's governance-boundary section, directly verified anchors for the **Analytic Tradecraft and Source Integrity** lane include [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2026e]; [Agency, 2009]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **Analytic Tradecraft and Source Integrity** for **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**. [237, 2026]; [266, 2026].

Curriculum topic spine: Red Cell Analysis and Adversarial Wargaming, **Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**, **Timeline Analysis and Event Sequencing**. **Verified anchor cluster:** [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2026e]; [Agency, 2009]; [for the Study of Intelligence, 2002]; [for the Study of Intelligence, 1994]; [Agency, 2016].

Conceptual depth: turning uncertainty into reviewable judgment through sourcing, alternatives, separated likelihood and confidence language, warning indicators, and explicit analytic lineage.

Method stack: key assumptions check, analysis of competing hypotheses, diagnosticity review, indicators and warnings, probability calibration, red-team review, collective tradecraft rating, and source descriptor audit.

Composability contract: every agent output must preserve evidence, assumptions, judgments, likelihood, confidence, dissent, empirical limits, and change history as separable fields.

Known failure modes: source laundering, automation bias, hidden assumptions, collapsed likelihood/confidence language, hindsight certainty, SAT-as-bias-cure overclaiming, and visually persuasive but weakly sourced claims.

Defensive boundary: analysis remains educational and decision-supportive; it does not become tasking, targeting, covert collection, or policy advocacy. Applied to **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**.

Anchor	Why it matters here
[of the Director of National Intelligence, 2015]	Official ODNI analytic tradecraft standards directive. Checked as of 2026-05-21; role: source_quality_anchor.
[of the Director of National Intelligence, 2026d]	Official sourcing directive for traceability, citations, source descriptors, and source summaries. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026e]	Official ODNI explanation of analytic objectivity, ombuds, and tradecraft standards. Checked as of 2026-05-21; role: curriculum_anchor.
[Agency, 2009]	Official structured analytic techniques primer for bias checks, alternatives, and warning analysis. Checked as of 2026-05-21; role: curriculum_anchor.
[for the Study of Intelligence, 2002]	Official CIA Center for the Study of Intelligence essay on Kent's professionalization of intelligence analysis and analytic standards. Checked as of 2026-06-11; role: curriculum_anchor.
[for the Study of Intelligence, 1994]	Official CIA CSI republication of Kent's final essay on analyst-policy relations, warning, intention, and communication boundaries. Checked as of 2026-06-11; role: curriculum_anchor.
[Agency, 2016]	Defense intelligence structured-analysis primer for classroom analytic exercises. Checked as of 2026-05-21; role: curriculum_anchor.

58.3.5.1 Advanced Analysis Methods evidence standard and citation floor: source families and discovery limits Official guidance supplies governance, safety, and legal constraints for the **Analytic Tradecraft and Source Integrity** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [237, 2026]; [266, 2026].

58.3.6 Advanced Analysis Methods agentic boundary: assist, approve, block, and record

Evidence anchor. Section 58; [237, 2026].

AGEINT translation is bounded by the **Analytic Tradecraft and Source Integrity** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**.

58.3.6.1 Advanced Analysis Methods permitted defensive utility: curriculum uses and safe outputs **Evidence anchor.** Section 58; [237, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**.

58.3.6.2 Advanced Analysis Methods excluded operational boundary: blocked actions and stop rules Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [237, 2026]; [266, 2026] and **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

58.3.7 Advanced Analysis Methods governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 58; [237, 2026].

Governance is practiced as a gate on the **Analytic Tradecraft and Source Integrity** lane. Learners use the **Structured-Judgment Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**.

58.3.7.1 Advanced Analysis Methods governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [237, 2026]; [266, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Analytic Tradecraft and Source Integrity** failure modes and the **Structured-Judgment Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

58.3.7.2 Advanced Analysis Methods evidence package handoff: appendices, records, and reuse **Evidence anchor.** Section 58; [237, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Structured-Judgment Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**.

58.3.7.3 Advanced Analysis Methods current-source assurance: verified anchors and local artifact fit The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**. [237, 2026]; [266, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_odni_icd_203` for **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**?	Intelligence Community Directive 203: Analytic Standards; lane `source_quality_spine`; checked 2026-05-21.	analytic note with hypotheses, evidence table, confidence, and dissent fields; Official ODNI analytic tradecraft standards directive.
What does the module inherit from `official_odni_icd_206` for **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**?	Intelligence Community Directive 206: Sourcing Requirements for Disseminated Analytic Products; lane `analytic_tradecraft`; checked 2026-05-21.	analytic note with hypotheses, evidence table, confidence, and dissent fields; Official sourcing directive for traceability, citations, source descriptors, and source summaries.
What does the module inherit from `official_odni_objectivity` for **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**?	Objectivity and IC Analytic Standards; lane `analytic_tradecraft`; checked 2026-05-21.	analytic note with hypotheses, evidence table, confidence, and dissent fields; Official ODNI explanation of analytic objectivity, ombuds, and tradecraft standards.
What does the module inherit from `official_cia_tradecraft_primer` for **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**?	A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis; lane `analytic_tradecraft`; checked 2026-05-21.	analytic note with hypotheses, evidence table, confidence, and dissent fields; Official structured analytic techniques primer for bias checks, alternatives, and warning analysis.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 58; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

58.3.8 Advanced Analysis Methods assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 58; [237, 2026].

58.3.9 Advanced Analysis Methods assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 58; [237, 2026].

58.3.9.1 Advanced Analysis Methods capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis** and [237, 2026]; [266, 2026].

58.3.9.2 Advanced Analysis Methods instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis** and [237, 2026]; [266, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

58.3.9.3 Advanced Analysis Methods assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Red Cell Analysis and Adversarial Wargaming	Completed **analytic note with hypotheses, evidence table, confidence, and dissent fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Network Analysis: Link Charts, Activity Matrices, Social Network Analysis	Completed **analytic note with hypotheses, evidence table, confidence, and dissent fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Timeline Analysis and Event Sequencing	Completed **analytic note with hypotheses, evidence table, confidence, and dissent fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

58.3.10 Advanced Analysis Methods refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [237, 2026]; [266, 2026] and **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**.

58.3.10.1 Advanced Analysis Methods refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**. The local signals begin with [237, 2026]; [266, 2026].

58.3.10.2 Advanced Analysis Methods claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**, and the source spine for these checks begins with [237, 2026]; [266, 2026].

58.3.11 Advanced Analysis Methods reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [237, 2026]; [266, 2026].

Triangulation anchors. In module 42's review-checklist section, directly verified anchors for the **Analytic Tradecraft and Source Integrity** lane include [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026d]; [of the Director of National Intelligence, 2026e]; [Agency, 2009]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis**. [237, 2026]; [266, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

58.3.12 Advanced Analysis Methods learning-path links: module map, overview, and curriculum atlas

Follow the cross-links to move between **Red Cell Analysis and Adversarial Wargaming; Network Analysis: Link Charts, Activity Matrices, Social Network Analysis** and the rest of the curriculum without losing the source spine: orientation first, then the parent unit, then the modules on either side. Primary sources: [237, 2026]; [266, 2026].

Section 2, Section 56, Section 57, Section 59

59 PRODUCTIVITY INTELLIGENCE AND COGNITIVE PERFORMANCE

59.1 PRODUCTIVITY INTELLIGENCE AND COGNITIVE PERFORMANCE learning spine and source route: unit purpose, module order, and evidence handoff

Evidence anchor. Section 59; [262, 2026].

59.1.1 analyst cognitive performance discipline spine: domain question and learning focus

Evidence anchor. Section 59; [262, 2026].
This unit teaches **analyst cognitive performance**. Productivity lessons frame workload, attention, external memory, handoffs, and review rhythm as quality controls for intelligence work.

59.1.2 analyst cognitive performance source-use contract: citation roles and evidence limits

Evidence anchor. Section 59; [262, 2026].
Use source-guide and governance anchors for records, review, accessibility, and accountable workflow claims.

59.1.3 analyst cognitive performance practice artifact: recurring packet and retained evidence

Evidence anchor. Section 59; [262, 2026].
The recurring practice artifact is a **workload and decision-hygiene card** that draws on workload signal, focus-block plan, handoff memo, and review checkpoint. The unit keeps its learning spine explicit. Learners identify overload, protect focus, preserve handoffs, and define re-entry context after interruption.

59.1.4 analyst cognitive performance safety boundary: accountable, synthetic, and evidence-bounded limits

No productivity optimization may override safety, review, accessibility, rest, or records duties.
This unit introduces the part's governing question, evidence artifacts, source-support spine, and capstone thread before the individual modules begin. [262, 2026]; [263, 2026].
Learners carry one unit capstone thread through the part: define an accountable intelligence question, bind it to source-quality constraints, produce a reviewable artifact, test the artifact against failure modes, and hand it off with enough context for another analyst or instructor to audit. The capstone remains public, synthetic, or owned-lab throughout; its first source anchors are [262, 2026]; [263, 2026].
This unit's deliverables are a source-canon card, claim/evidence ledger, safe-practice lab packet, failure-mode note, instructor rubric, and debrief memo. The full source-lane and evidence-package ledgers appear in the orientation and appendices; this unit introduction keeps only the learner-facing spine for [262, 2026]; [263, 2026].
This unit's safety gates are scope authorization, rights review, data provenance, tool allowlisting, human oversight, rollback, and evidence-bounded output. A missing gate turns the activity into a tabletop, audit, or written governance exercise until the gate is restored against [262, 2026]; [263, 2026].
Capstone thread:

Phase	Artifact	Review gate
Question	accountable learning question and excluded-action list	instructor confirms scope, allowed data, and rights impact
Source canon	source-lane map with guide citations, verified anchors, and refresh dates	citation keys resolve and source identity lock remains stable
Evidence ledger	claim, evidence, uncertainty, confidence, and reviewer register	every material claim has a source, caveat, and owner
Safe lab	synthetic or public dataset packet, tool allowlist, and stop conditions	no live target, private data, external action, or unsafe cyber-physical step
Assurance	evaluation rubric, failure-mode drill, rights map, and remediation note	human reviewer signs off before presentation or reuse
Debrief	capstone memo with lessons, residual risk, refresh triggers, and handoff owner	all unresolved questions and future approvals are explicit

Research lane: Operator Productivity and Cognitive Performance. Core anchors: [of the Director of National Intelligence, 2015]; [Jr., 2007]; [of Standards and Technology, 2022c]. Conceptual focus: sustained intelligence work as cognitive performance engineering: external memory, workload measurement, flow conditions, and decision hygiene under operational tempo. Composability contract: requirements queues, workload signals, focus blocks, evidence packets, and reviewer checkpoints remain separable artifacts. **Practice lens:** Dissemination-and-Marking Control Lens; Which audience, release authority, marking vocabulary, records duty, and feedback loop governs this intelligence artifact? [262, 2026]; [263, 2026].

59.1.5 PRODUCTIVITY INTELLIGENCE AND COGNITIVE PERFORMANCE visual navigation and module map: evidence flow, order, and safety cues

The unit uses Figure 129 and Figure 130 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 58, Section 60.

59.1.6 PRODUCTIVITY INTELLIGENCE AND COGNITIVE PERFORMANCE module roster and source-lane inventory: citations, lanes, and learner route

Module	Section reference	Source spine
The Intelligent Operator as Cognitive Athlete	Section 60	[262, 2026]; [263, 2026]; [264, 2026]; [278, 2026]; [279, 2026]; [283, 2026]; [290, 2026]; [291, 2026]; [294, 2026]; [197, 2026]; [198, 2026]; [199, 2026]; [179, 2026]; [200, 2026]; [201, 2026]; [202, 2026]; [203, 2026]; [204, 2026]; [205, 2026]; [206, 2026]; [207, 2026]; [025, 2026]; [297, 2026]; [298, 2026]; [308, 2026]; [311, 2026]; [300, 2026]; [304, 2026]; [306, 2026].

Module	Section reference	Source spine
Information Architecture for Intelligence Work	Section 61	[251, 2026]; [268, 2026]; [269, 2026]; [280, 2026]; [281, 2026]; [282, 2026]; [292, 2026]; [295, 2026]; [296, 2026]; [308, 2026]; [311, 2026]; [307, 2026]; [305, 2026]; [304, 2026]; [052, 2026]; [051, 2026]; [297, 2026]; [298, 2026]; [055, 2026]; [301, 2026]; [309, 2026]; [310, 2026]; [300, 2026].

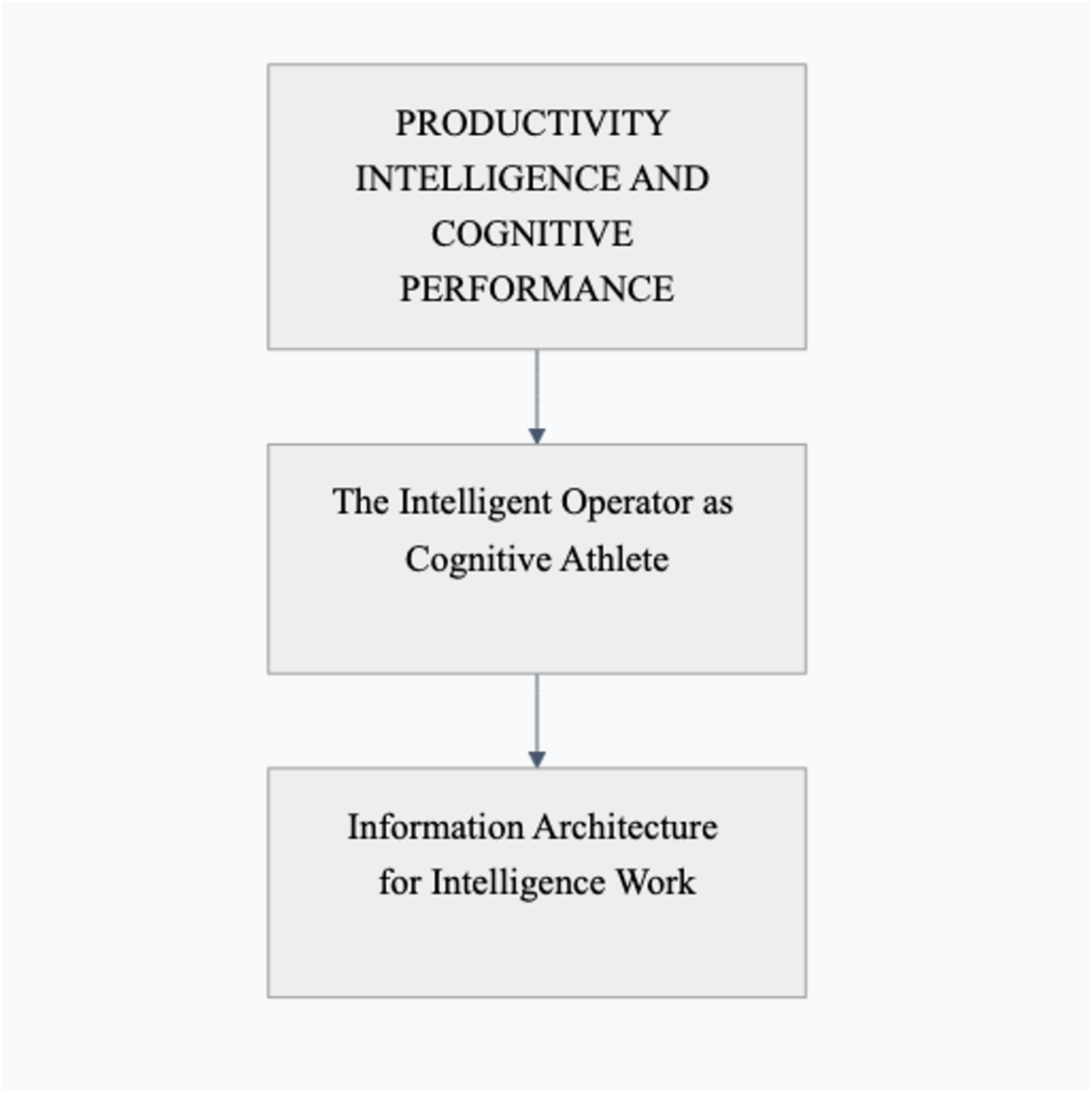


Figure 129: The unit module map traces the part's chapters as a linear reading sequence. It is anchored to the productivity intelligence and cognitive performance section; use it to inspect 2 module nodes in the unit's ordered, source-backed reading sequence from its first module to its last while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

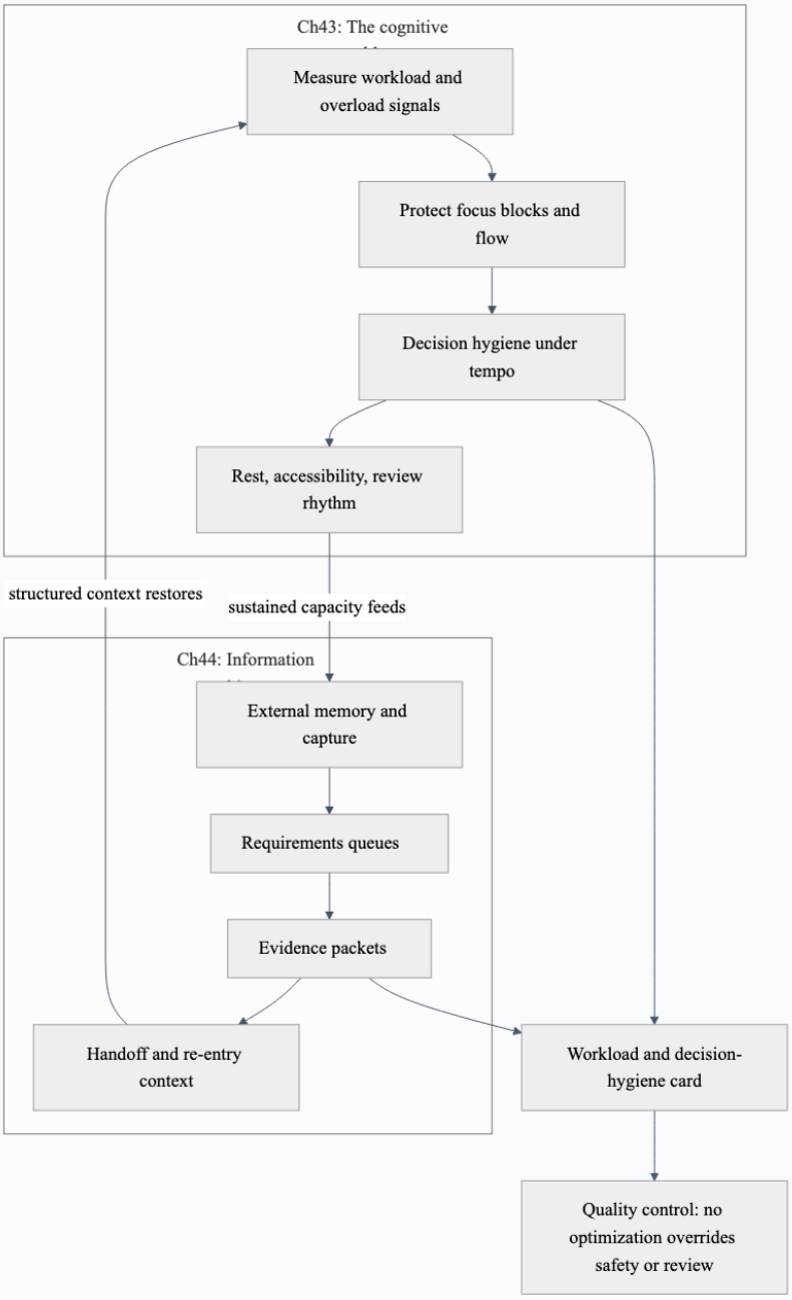


Figure 130: This part frames sustained intelligence work as two coupled loops — the cognitive athlete who manages workload, focus, and decision hygiene, and the information architecture that externalizes memory and preserves handoffs — both feeding a workload-and-decision-hygiene card gated so no optimization overrides safety or review.

60 The Intelligent Operator as Cognitive Athlete

60.0.1 The Intelligent Operator as Cognitive Athlete figures and course links: visual evidence, source flow, and navigation

The module uses Figure 131 and Figure 129 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.

Navigation links: Section 2, Section 59, Section 61.

This module teaches the **Operator Productivity and Cognitive Performance** lane through a bounded, source-backed coursebook chapter. [262, 2026]; [263, 2026].

60.1 Operator Productivity and Cognitive Performance frame for The Intelligent Operator as Cognitive Athlete: source context, topic focus, and reader task

Evidence anchor. Section 60; [262, 2026].

60.1.1 The Intelligent Operator as Cognitive Athlete orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 60; [262, 2026].

60.1.2 The Intelligent Operator as Cognitive Athlete conceptual primer: source context, core model, and reader task

This chapter teaches intelligence productivity as governed cognitive performance: external memory, workload limits, flow conditions, and explicit review handoffs keep judgment reliable under sustained tempo. The chapter uses **Operator-Workload Hygiene Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations**.

The central distinction is to separate cognitive hygiene from heroics, and workload signals from unreviewed urgency. Core topics include **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done (GTD): Cognitive Foundations; GTD as External Memory and Affordance System**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.

Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [of the Director of National Intelligence, 2015]; [Jr., 2007]; [of Standards and Technology, 2022c]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [262, 2026]; [263, 2026].

Learners move from vocabulary and the **Operator-Workload Hygiene Lens** distinction through topic lessons on **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations** with evidence and misconception checks, then assemble an **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** with safety and rights gates.

60.1.3 The Intelligent Operator as Cognitive Athlete learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 60; [262, 2026].

- Connect **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations and The Science Behind Getting Things Done (GTD): Cognitive Foundations** to **Operator Productivity and Cognitive Performance** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build an **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate cognitive hygiene from heroics, and workload signals from unreviewed urgency; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as heroic overtime, invisible cognitive debt, context-switch thrash, uncalibrated confidence under load, and skipping handoff review, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: productivity material stays educational and synthetic; it does not prescribe live operational tempo, surveillance of people, or performance coercion.

60.1.4 The Intelligent Operator as Cognitive Athlete core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 60; [262, 2026].

Term	Working definition
External memory	a trusted capture system that holds tasks and commitments outside working memory
NASA-TLX	a subjective workload instrument for rating mental, temporal, and effort demands
Flow precondition	task clarity, challenge-skill balance, and feedback that enable focused work
Decision hygiene	habits that preserve evidence review, handoffs, and rest boundaries under load
Task switching	context change with measurable recovery cost and explicit re-entry notes
Productivity Tradecraft: Managing Cognitive…	Key terms: Productivity, Tradecraft, Managing.
The Science Behind Getting Things Done (GTD):…	Key terms: Science, Behind, Getting.

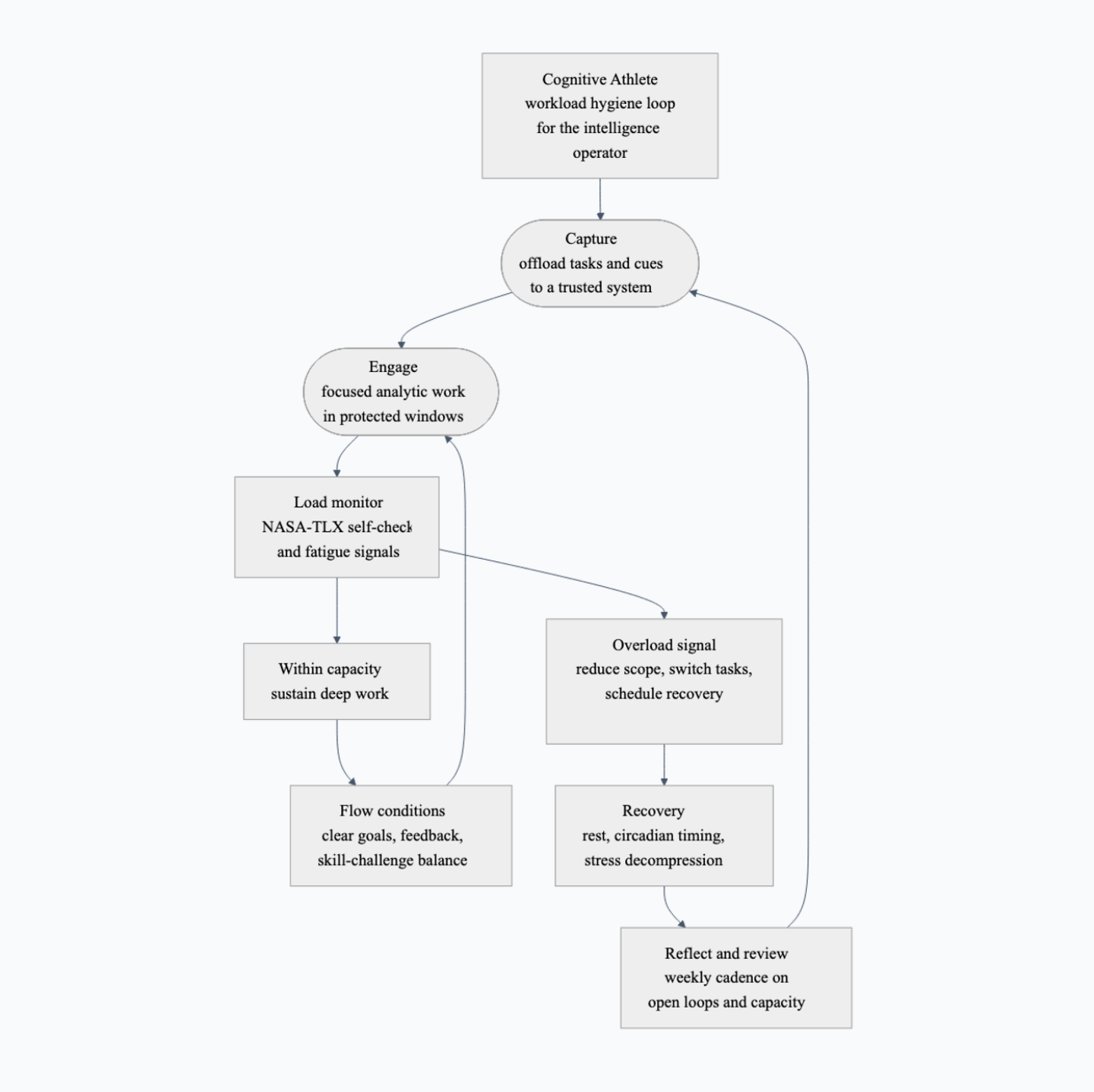


Figure 131: This diagram teaches how an intelligence operator sustains performance by capturing open loops, protecting focus, monitoring cognitive load, and routing overload into deliberate recovery. In the productivity intelligence and cognitive performance / the intelligent operator as cognitive athlete section, it lets readers compare Cognitive Athlete workload hygiene loop for the intelligence operator, Capture offload tasks and cues to a trusted system, Engage focused analytic work in protected windows, and Load monitor NASA-TLX self-check and fatigue signals so the visual functions as a traceable course aid rather than an unscoped assertion.

60.2 Operator-Workload Hygiene Lens path for The Intelligent Operator as Cognitive Athlete: lesson cluster, safe artifact, and review

Evidence anchor. Section 60; [262, 2026].

60.2.1 The Intelligent Operator as Cognitive Athlete practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 60; [262, 2026].

60.2.2 The Intelligent Operator as Cognitive Athlete topic lessons: source-backed concepts and transfer tasks

This module builds intelligence productivity as governed cognitive performance: external memory, workload limits, flow conditions, and explicit review handoffs keep judgment reliable under sustained tempo. The sequence opens with **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations**, **The Science Behind Getting Things Done (GTD): Cognitive Foundations**, **GTD as External Memory and Affordance System** and applies the **Operator-Workload Hygiene Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 129; module overview Section 60; curriculum atlas Section 2.

Triangulation anchors. In module 43's topic-lessons section, directly verified anchors for the **Operator Productivity and Cognitive Performance** lane include [of the Director of National Intelligence, 2015]; [Jr., 2007]; [of Standards and Technology, 2022c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

60.2.2.1 Lesson 1: Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations

Concept. **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations** manages workload and bias through prioritization, explicit handoffs, and review checkpoints—not unsustainable pace.

Why it matters. **Productivity Tradecraft** connects classroom vocabulary to Operator Productivity and Cognitive Performance practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations** rests on [308, 2026] and [311, 2026]. The closest source to this row notes: It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering. Use them for the working definition that **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of the Director of National Intelligence, 2015]; [Jr., 2007].

Evidence to inspect. Read **Productivity Tradecraft** against the works cited for this row. [308, 2026] An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure. [311, 2026] An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Productivity Tradecraft**, build a **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** for this workload-aware operator decision hygiene topic. The artifact must note the workload descriptor, the bounded claim about **Productivity Tradecraft**, the fatigue caveat, the uncertainty margin, the do-not-escalate boundary, and the reviewer who owns the handoff. Shape **Productivity Tradecraft** work as a **workload and decision-hygiene card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Productivity Tradecraft**: that feeling certain in the moment substitutes for the checklist, pause, and second-look that decision hygiene exists to enforce.

Transfer task. Apply this module's safe boundary for **Productivity Tradecraft** to another artifact while keeping workload-aware operator decision hygiene and reviewer ownership explicit.

60.2.2.2 Lesson 2: The Science Behind Getting Things Done (GTD): Cognitive Foundations

Concept. **The Science Behind Getting Things Done (GTD): Cognitive Foundations** uses GTD as a decision-hygiene framework: capture, clarify, organize, review, and engage—with explicit authority for what enters analysis.

Why it matters. Without explicit treatment of **The Science Behind Getting Things Done (GTD)**, heroic overtime undermines workload-aware operator decision hygiene review; the lesson builds the habit to separate cognitive hygiene from heroics, and workload signals from unreviewed urgency.

Source support. **The Science Behind Getting Things Done (GTD): Cognitive Foundations** rests on [197, 2026]. Its anchor reference records: In 2001 David Allen proposed 'Getting Things Done' (GTD) as a method for enhancing personal. Use it for fixing what **The Science Behind Getting Things Done (GTD): Cognitive Foundations** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of the Director of National Intelligence, 2015]; [Jr., 2007].

Evidence to inspect. Ground **The Science Behind Getting Things Done (GTD)** in the evidence the row cites. [197, 2026] In 2001 David Allen proposed 'Getting Things Done' (GTD) as a method for enhancing personal. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **The Science Behind Getting Things Done (GTD)**, build a **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** for this workload-aware operator decision hygiene topic. The artifact must note the workload descriptor, the bounded claim about **Science Behind Getting Things Done**, the fatigue caveat, the uncertainty margin, the do-not-escalate boundary, and the reviewer who owns the handoff. Shape **The Science Behind Getting Things Done (GTD)** work as a **workload and decision-hygiene card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **The Science Behind Getting Things Done (GTD)**: that feeling certain in the moment substitutes for the checklist, pause, and second-look that decision hygiene exists to enforce.

Transfer task. Transfer **The Science Behind Getting Things Done (GTD)** from this module to a second motif by preserving workload-aware operator decision hygiene, replacing action with audit, and naming the blocked use.

60.2.2.3 Lesson 3: GTD as External Memory and Affordance System

Concept. **GTD as External Memory and Affordance System** connects cognitive science claims to analytic bias literacy: what the brain prioritizes, what it misses, and how review compensates.

Why it matters. Analysts use **GTD as External Memory and Affordance System** to separate cognitive hygiene from heroics, and workload signals from unreviewed urgency. A defensible treatment names the judgment it enables for workload-aware operator decision hygiene review, the proof limit that heroic overtime would otherwise hide, and the reviewer accountable for challenge.

Source support. **GTD as External Memory and Affordance System** rests on [197, 2026]. The closest source to this row notes: In 2001 David Allen proposed 'Getting Things Done' (GTD) as a method for enhancing personal. Use it for the working definition that **GTD as External Memory and Affordance System** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of the Director of National Intelligence, 2015]; [Jr., 2007].

Evidence to inspect. For **GTD as External Memory and Affordance System**, reason from the sources cited in this row. [197, 2026] In 2001 David Allen proposed 'Getting Things Done' (GTD) as a method for enhancing personal. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **GTD as External Memory and Affordance System**, build a **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** for this workload-aware operator decision hygiene topic. The artifact must note the workload descriptor, the bounded claim about **GTD as External Memory and**, the fatigue caveat, the uncertainty margin, the do-not-escalate boundary, and the reviewer who owns the handoff. Shape this subject work as a **workload and decision-hygiene card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **GTD as External Memory and Affordance System**: that feeling certain in the moment substitutes for the checklist, pause, and second-look that decision hygiene exists to enforce.

Transfer task. Apply this module's safe boundary for **GTD as External Memory and Affordance System** to another artifact while keeping workload-aware operator decision hygiene and reviewer ownership explicit.

60.2.2.4 Lesson 4: The Five GTD Phases: Capture, Clarify, Organize, Reflect, Engage

Concept. The Five GTD Phases: Capture, Clarify, Organize, Reflect, Engage uses GTD as a decision-hygiene framework: capture, clarify, organize, review, and engage—with explicit authority for what enters analysis.

Why it matters. Without explicit treatment of **The Five GTD Phases**, heroic overtime undermines workload-aware operator decision hygiene review; the lesson builds the habit to separate cognitive hygiene from heroics, and workload signals from unreviewed urgency.

Source support. The Five GTD Phases: Capture, Clarify, Organize, Reflect, Engage rests on [198, 2026]. The closest source to this row notes: The page also surveys software tools for implementing GTD, such as Todoist, OmniFocus, Trello, Evernote, and Notion. Use it for the working definition that **The Five GTD Phases: Capture, Clarify, Organize, Reflect, Engage** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of the Director of National Intelligence, 2015]; [Jr., 2007].

Evidence to inspect. Read **The Five GTD Phases** against the works cited for this row. [198, 2026] A Czech-language explainer of the Getting Things Done (GTD) productivity method created by David Allen. It describes the system's core steps of capturing thoughts, clarifying them into actionable items, organizing and prioritizing, regularly reviewing, and executing, including the principle of doing any task that takes under two minutes immediately. The page also surveys software tools for implementing GTD, such as Todoist, OmniFocus, Trello, Evernote, and Notion. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **The Five GTD Phases**, build a **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** for this workload-aware operator decision hygiene topic. The artifact must note the workload descriptor, the bounded claim about **Five GTD Phases**, the fatigue caveat, the uncertainty margin, the do-not-escalate boundary, and the reviewer who owns the handoff. Shape **The Five GTD Phases** work as a **workload and decision-hygiene card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **The Five GTD Phases**: that feeling certain in the moment substitutes for the checklist, pause, and second-look that decision hygiene exists to enforce.

Transfer task. Apply this module's safe boundary for **The Five GTD Phases** to another artifact while keeping workload-aware operator decision hygiene and reviewer ownership explicit.

60.2.2.5 Lesson 5: Why GTD Improves Team Intelligence Performance (Allen, 2024)

Concept. Why GTD Improves Team Intelligence Performance (Allen, 2024) uses GTD as a decision-hygiene framework: capture, clarify, organize, review, and engage—with explicit authority for what enters analysis.

Why it matters. Analysts use **Why GTD Improves Team Intelligence Performance (Allen, 2024)** to separate cognitive hygiene from heroics, and workload signals from unreviewed urgency. A defensible treatment names the judgment it enables for workload-aware operator decision hygiene review, the proof limit that heroic overtime would otherwise hide, and the reviewer accountable for challenge.

Source support. Why GTD Improves Team Intelligence Performance (Allen, 2024) rests on [199, 2026]. Use it for fixing what **Why GTD Improves Team Intelligence Performance (Allen, 2024)** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of the Director of National Intelligence, 2015]; [Jr., 2007].

Evidence to inspect. Read **Why GTD Improves Team Intelligence Performance (Allen, 2024)** against the works cited for this row. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Why GTD Improves Team Intelligence Performance (Allen, 2024)**, build a **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** for this workload-aware operator decision hygiene topic. The artifact must note the workload descriptor, the bounded claim about **Why GTD Improves Team Intelligence**, the fatigue caveat, the uncertainty margin, the do-not-escalate boundary, and the reviewer who owns the handoff. Shape this subject work as a **workload and decision-hygiene card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Why GTD Improves Team Intelligence Performance (Allen, 2024)**: that feeling certain in the moment substitutes for the checklist, pause, and second-look that decision hygiene exists to enforce.

Transfer task. Transfer **Why GTD Improves Team Intelligence Performance (Allen, 2024)** from this module to a second motif by preserving workload-aware operator decision hygiene, replacing action with audit, and naming the blocked use.

60.2.2.6 Lesson 6: GTD and Reduction of Cognitive Load: Empirical Evidence

Concept. GTD and Reduction of Cognitive Load: Empirical Evidence manages analyst workload through prioritization, checklists, rest boundaries, and explicit handoff—not heroics.

Why it matters. GTD and Reduction of Cognitive Load matters in the **Operator Productivity and Cognitive Performance** lane because workload-aware operator decision hygiene evidence must stay separate from judgment; heroic overtime is a common failure.

Source support. GTD and Reduction of Cognitive Load: Empirical Evidence rests on [179, 2026] and [197, 2026]. The lead source's own note reads: An NCSU Laboratory for Analytic Sciences article summarizing a systematic survey of metrics for measuring cognitive load in intelligence-analysis and similar settings. Use them for the working definition that **GTD and Reduction of Cognitive Load: Empirical Evidence** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of the Director of National Intelligence, 2015]; [Jr., 2007].

Evidence to inspect. For **GTD and Reduction of Cognitive Load**, work from the cited evidence behind this row. [179, 2026] An NCSU Laboratory for Analytic Sciences article summarizing a systematic survey of metrics for measuring cognitive load in intelligence-analysis and similar settings. Reviewing 125 articles published between 1998 and 2024, it identifies 129 distinct metrics grouped into non-biometric methods (questionnaires such as NASA-TLX, task performance, interaction tracking) and biometric methods (eye tracking, heart rate). [197, 2026] In 2001 David Allen proposed 'Getting Things Done' (GTD) as a method for enhancing personal. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **GTD and Reduction of Cognitive Load**, build a **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** for this workload-aware operator decision hygiene topic. The artifact must note the workload descriptor, the bounded claim about **GTD and Reduction of Cognitive**, the fatigue caveat, the uncertainty margin, the do-not-escalate boundary, and the reviewer who owns the handoff. Shape **GTD and Reduction of Cognitive Load** work as a **workload and decision-hygiene card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **GTD and Reduction of Cognitive Load**: that feeling certain in the moment substitutes for the checklist, pause, and second-look that decision hygiene exists to enforce.

Transfer task. Reuse the **GTD and Reduction of Cognitive Load** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

60.2.2.7 Lesson 7: Flow State and Peak Performance in Intelligence Work

Concept. Flow State and Peak Performance in Intelligence Work treats flow claims as operator-performance literacy: define task clarity, feedback, and review boundaries—not unsustainable pace.

Why it matters. Analysts use **Flow State and Peak Performance in Intelligence Work** to separate cognitive hygiene from heroics, and workload signals from unreviewed urgency. A defensible treatment names the judgment it enables for workload-aware operator decision hygiene review, the proof limit that heroic overtime would otherwise hide, and the reviewer accountable for challenge.

Source support. Flow State and Peak Performance in Intelligence Work rests on [200, 2026], [201, 2026], and [202, 2026]. The most specific cited work observes: The authors argue that the dopamine and norepinephrine systems drive the motivational and mood components of flow, and that interaction among the default mode, central executive, and salience networks produces its characteristic features. Use them for fixing what **Flow State and Peak Performance in Intelligence Work** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of the Director of National Intelligence, 2015]; [Jr., 2007].

Evidence to inspect. Read **Flow State and Peak Performance in Intelligence Work** against the works cited for this row. [200, 2026] A marketing blog post on the Dingbats Notebooks e-commerce site about flow state and how writing tools can support it. It summarizes Mihaly Csikszentmihalyi's concept of flow as a state of full absorption marked by intense focus, clear goals, and immediate feedback, and reviews associated benefits and neuroscience such as reduced prefrontal-cortex activity and increased dopamine. [201, 2026] A 2020 theoretical review article in the European Journal of Neuroscience by van der Linden, Tops, and Bakker proposing a neuroscientific model of flow, the state of full task absorption with strong drive and low self-referential thinking. The authors argue that the dopamine and norepinephrine systems drive the motivational and mood components of flow, and that interaction among the default mode, central executive, and salience networks produces its characteristic features. [202, 2026] A Wikipedia article on flow, the psychological state of complete immersion and focused engagement in an activity, also known as being in the zone. It traces the concept to psychologist Mihaly Csikszentmihalyi and describes flow as a balance between challenge and skill, characterized by intense concentration, merging of action and awareness, loss of self-consciousness, a sense of control, distorted time perception, and intrinsic reward. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Flow State and Peak Performance in Intelligence Work**, build a **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** for this workload-aware operator decision hygiene topic. The artifact must note the workload descriptor, the bounded claim about **Flow State and Peak Performance**, the fatigue caveat, the uncertainty margin, the do-not-escalate boundary, and the reviewer who owns the handoff. Shape this subject work as a **workload and decision-hygiene card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Flow State and Peak Performance in Intelligence Work**: that feeling certain in the moment substitutes for the checklist, pause, and second-look that decision hygiene exists to enforce.

Transfer task. Apply this module's safe boundary for **Flow State and Peak Performance in Intelligence Work** to another artifact while keeping workload-aware operator decision hygiene and reviewer ownership explicit.

60.2.2.8 Lesson 8: Csikszentmihalyi's Flow: Definition, Seven Conditions, Neurophysiology

Concept. Csikszentmihalyi's Flow: Definition, Seven Conditions, Neurophysiology treats flow claims as operator-performance literacy: define task clarity, feedback, and review boundaries—not unsustainable pace.

Why it matters. Without explicit treatment of **Csikszentmihalyi's Flow**, heroic overtime undermines workload-aware operator decision hygiene review; the lesson builds the habit to separate cognitive hygiene from heroics, and workload signals from unreviewed urgency.

Source support. Csikszentmihalyi's Flow: Definition, Seven Conditions, Neurophysiology rests on [203, 2026]. The lead source's own note reads: The piece argues that achieving flow states enhances productivity and job satisfaction across roles and industries. Use it for fixing what **Csikszentmihalyi's Flow: Definition, Seven Conditions, Neurophysiology** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of the Director of National Intelligence, 2015]; [Jr., 2007].

Evidence to inspect. For **Csikszentmihalyi's Flow**, reason from the sources cited in this row. [203, 2026] A blog article applying Mihaly Csikszentmihalyi's Flow Theory to workplace and career performance. It describes flow as a state of full absorption in an activity, lists conditions associated with it such as clear goals, immediate feedback, and a balance between challenge and skill, and discusses how time can appear distorted during flow. The piece argues that achieving flow states enhances productivity and job satisfaction across roles and industries. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Csikszentmihalyi's Flow**, build a **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** for this workload-aware operator decision hygiene topic. The artifact must note the workload descriptor, the bounded claim about **Csikszentmihalyi's Flow**, the fatigue caveat, the uncertainty margin, the do-not-escalate boundary, and the reviewer who owns the handoff. Shape **Csikszentmihalyi's Flow** work as a **workload and decision-hygiene card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Csikszentmihalyi's Flow**: that feeling certain in the moment substitutes for the checklist, pause, and second-look that decision hygiene exists to enforce.

Transfer task. Reuse the **Csikszentmihalyi's Flow** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

60.2.2.9 Lesson 9: Neuroscience of Flow: Prefrontal Cortex Deactivation, Dopamine

Concept. Neuroscience of Flow: Prefrontal Cortex Deactivation, Dopamine manages workload and bias through prioritization, explicit handoffs, and review checkpoints—not unsustainable pace.

Why it matters. Neuroscience of Flow connects classroom vocabulary to Operator Productivity and Cognitive Performance practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Neuroscience of Flow: Prefrontal Cortex Deactivation, Dopamine rests on [204, 2026]. The lead source's own note reads: It describes brain mechanisms associated with flow, including reduced prefrontal activity (transient hypofrontality) that lowers self-consciousness, dopamine-driven motivation, and deactivation of the default mode network to enable deep focus. Use it for the working definition that **Neuroscience of Flow: Prefrontal Cortex Deactivation, Dopamine** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of the Director of National Intelligence, 2015]; [Jr., 2007].

Evidence to inspect. Ground **Neuroscience of Flow** in the evidence the row cites. [204, 2026] A LinkedIn article (Sana Noor, 2024) on the neuroscience of flow, the state of complete immersion in a task. It describes brain mechanisms associated with flow, including reduced prefrontal activity (transient hypofrontality) that lowers self-consciousness, dopamine-driven motivation, and deactivation of the default mode network to enable deep focus. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Neuroscience of Flow**, build a **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** for this workload-aware operator decision hygiene topic. The artifact must note the workload descriptor, the bounded claim about **Neuroscience of Flow**, the fatigue caveat, the uncertainty margin, the do-not-escalate boundary, and the reviewer who owns

the handoff. Shape **Neuroscience of Flow** work as a **workload and decision-hygiene card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Neuroscience of Flow**: that feeling certain in the moment substitutes for the checklist, pause, and second-look that decision hygiene exists to enforce.

Transfer task. Transfer **Neuroscience of Flow** from this module to a second motif by preserving workload-aware operator decision hygiene, replacing action with audit, and naming the blocked use.

60.2.2.10 Lesson 10: Flow Research Collective Concept. Flow Research Collective manages workload and bias through prioritization, explicit handoffs, and review checkpoints—not unsustainable pace.

Why it matters. Flow Research Collective connects classroom vocabulary to Operator Productivity and Cognitive Performance practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Flow Research Collective rests on [205, 2026]. Its anchor reference records: This is the website of the Flow Research Collective, a research and development organization founded in 2018 that studies the neuroscience of human performance and brain health. Use it for the working definition that **Flow Research Collective** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of the Director of National Intelligence, 2015]; [Jr., 2007].

Evidence to inspect. Read **Flow Research Collective** against the works cited for this row. [205, 2026] This is the website of the Flow Research Collective, a research and development organization founded in 2018 that studies the neuroscience of human performance and brain health. It investigates flow states of focused absorption and applies that research to peak performance training for organizations as well as to mental health conditions such as PTSD and depression. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. Build a **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** for this workload-aware operator decision hygiene topic. The artifact must note the workload descriptor, the bounded claim about **Flow Research Collective**, the fatigue caveat, the uncertainty margin, the do-not-escalate boundary, and the reviewer who owns the handoff. Shape this subject work as a **workload and decision-hygiene card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Flow Research Collective**: that feeling certain in the moment substitutes for the checklist, pause, and second-look that decision hygiene exists to enforce.

Transfer task. Apply this module's safe boundary for **Flow Research Collective** to another artifact while keeping workload-aware operator decision hygiene and reviewer ownership explicit.

60.2.2.11 Lesson 11: Go With the Flow: Neuroscientific View on Full Engagement (PMC, 2020) Concept. Go With the Flow: Neuroscientific View on Full Engagement (PMC, 2020) manages workload and bias through prioritization, explicit handoffs, and review checkpoints—not unsustainable pace.

Why it matters. Without explicit treatment of **Go With the Flow: Neuroscientific View on Full Engagement (PMC, 2020)**, heroic overtime undermines workload-aware operator decision hygiene review; the lesson builds the habit to separate cognitive hygiene from heroics, and workload signals from unreviewed urgency.

Source support. Go With the Flow: Neuroscientific View on Full Engagement (PMC, 2020) rests on [201, 2026]. Its anchor reference records: A 2020 theoretical review article in the European Journal of Neuroscience by van der Linden, Tops, and Bakker proposing a neuroscientific model of flow, the state of full task absorption with strong drive and low self-referential thinking. Use it for the claim that **Go With the Flow: Neuroscientific View on Full Engagement (PMC, 2020)** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of the Director of National Intelligence, 2015]; [Jr., 2007].

Evidence to inspect. For **Go With the Flow: Neuroscientific View on Full Engagement (PMC, 2020)**, work from the cited evidence behind this row. [201, 2026] A 2020 theoretical review article in the European Journal of Neuroscience by van der Linden, Tops, and Bakker proposing a neuroscientific model of flow, the state of full task absorption with strong drive and low self-referential thinking. The authors argue that the dopamine and norepinephrine systems drive the motivational and mood components of flow, and that interaction among the default mode, central executive, and salience networks produces its characteristic features. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Go With the Flow**, build a **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** for this workload-aware operator decision hygiene topic. The artifact must note the workload descriptor, the bounded claim about **Go With the Flow**, the fatigue caveat, the uncertainty margin, the do-not-escalate boundary, and the reviewer who owns the handoff. Shape **Go With the Flow: Neuroscientific View on Full Engagement (PMC, 2020)** work as a **workload and decision-hygiene card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Go With the Flow: Neuroscientific View on Full Engagement (PMC, 2020)**: that feeling certain in the moment substitutes for the checklist, pause, and second-look that decision hygiene exists to enforce.

Transfer task. Apply this module's safe boundary for **Go With the Flow: Neuroscientific View on Full Engagement (PMC, 2020)** to another artifact while keeping workload-aware operator decision hygiene and reviewer ownership explicit.

60.2.2.12 Lesson 12: Investigating the Flow Experience: Key Conceptual Issues (PMC, 2020) Concept. Investigating the Flow Experience: Key Conceptual Issues (PMC, 2020) treats flow claims as operator-performance literacy: define task clarity, feedback, and review boundaries—not unsustainable pace.

Why it matters. Investigating the Flow Experience connects classroom vocabulary to Operator Productivity and Cognitive Performance practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Investigating the Flow Experience: Key Conceptual Issues (PMC, 2020) rests on [206, 2026]. The most specific cited work observes: It identifies disagreements over whether flow is a discrete state or a continuum, whether enjoyment is essential to it, and whether scales conflate flow's conditions with the experience itself. Use it for the working definition that **Investigating the Flow Experience: Key Conceptual Issues (PMC, 2020)** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of the Director of National Intelligence, 2015]; [Jr., 2007].

Evidence to inspect. For **Investigating the Flow Experience**, work from the cited evidence behind this row. [206, 2026] A 2020 conceptual analysis by Sami Abuhamdeh in Frontiers in Psychology arguing that flow research has stalled because the construct is operationalized inconsistently across studies. It identifies disagreements over whether flow is a discrete state or a continuum, whether enjoyment is essential to it, and whether scales conflate flow's conditions with the experience itself. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Investigating the Flow Experience**, build a **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** for this workload-aware operator decision hygiene topic. The artifact must note the workload descriptor, the bounded claim about **Investigating the Flow Experience**, the fatigue caveat, the uncertainty margin, the do-not-escalate boundary, and the reviewer who owns the handoff. Shape **Investigating the Flow Experience** work as a **workload and decision-hygiene card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Investigating the Flow Experience**: that feeling certain in the moment substitutes for the checklist, pause, and second-look that decision hygiene exists to enforce.

Transfer task. Apply this module's safe boundary for **Investigating the Flow Experience** to another artifact while keeping workload-aware operator decision hygiene and reviewer ownership explicit.

60.2.2.13 Lesson 13: Engineering Flow State for Intelligence Analysis Environments

Concept. Engineering Flow State for Intelligence Analysis Environments treats flow claims as operator-performance literacy: define task clarity, feedback, and review boundaries—not unsustainable pace.

Why it matters. Engineering Flow State matters in the **Operator Productivity and Cognitive Performance** lane because workload-aware operator decision hygiene evidence must stay separate from judgment; heroic overtime is a common failure.

Source support. Engineering Flow State for Intelligence Analysis Environments rests on [205, 2026]. Its anchor reference records: It investigates flow states of focused absorption and applies that research to peak performance training for organizations as well as to mental health conditions such as PTSD and depression. Use it for the working definition that **Engineering Flow State for Intelligence Analysis Environments** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of the Director of National Intelligence, 2015]; [Jr., 2007].

Evidence to inspect. For **Engineering Flow State**, work from the cited evidence behind this row. [205, 2026] This is the website of the Flow Research Collective, a research and development organization founded in 2018 that studies the neuroscience of human performance and brain health. It investigates flow states of focused absorption and applies that research to peak performance training for organizations as well as to mental health conditions such as PTSD and depression. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Engineering Flow State**, build a **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** for this workload-aware operator decision hygiene topic. The artifact must note the workload descriptor, the bounded claim about **Engineering Flow State for Intelligence**, the fatigue caveat, the uncertainty margin, the do-not-escalate boundary, and the reviewer who owns the handoff. Shape **Engineering Flow State** work as a **workload and decision-hygiene card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Engineering Flow State**: that feeling certain in the moment substitutes for the checklist, pause, and second-look that decision hygiene exists to enforce.

Transfer task. Reuse the **Engineering Flow State** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

60.2.2.14 Lesson 14: Cognitive Load Management in Intelligence Work

Concept. Cognitive Load Management in Intelligence Work manages analyst workload through prioritization, checklists, rest boundaries, and explicit handoff—not heroics.

Why it matters. Cognitive Load Management connects classroom vocabulary to Operator Productivity and Cognitive Performance practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Cognitive Load Management in Intelligence Work rests on [179, 2026]. Its anchor reference records: An NCSU Laboratory for Analytic Sciences article summarizing a systematic survey of metrics for measuring cognitive load in intelligence-analysis and similar settings. Use it for the working definition that **Cognitive Load Management in Intelligence Work** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of the Director of National Intelligence, 2015]; [Jr., 2007].

Evidence to inspect. Ground **Cognitive Load Management** in the evidence the row cites. [179, 2026] An NCSU Laboratory for Analytic Sciences article summarizing a systematic survey of metrics for measuring cognitive load in intelligence-analysis and similar settings. Reviewing 125 articles published between 1998 and 2024, it identifies 129 distinct metrics grouped into non-biometric methods (questionnaires such as NASA-TLX, task performance, interaction tracking) and biometric methods (eye tracking, heart rate). Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Cognitive Load Management**, build a **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** for this workload-aware operator decision hygiene topic. The artifact must note the workload descriptor, the bounded claim about **Cognitive Load Management in Intelligence**, the fatigue caveat, the uncertainty margin, the do-not-escalate boundary, and the reviewer who owns the handoff. Shape **Cognitive Load Management** work as a **workload and decision-hygiene card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Cognitive Load Management**: that feeling certain in the moment substitutes for the checklist, pause, and second-look that decision hygiene exists to enforce.

Transfer task. Reuse the **Cognitive Load Management** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

60.2.2.15 Lesson 15: Cognitive Load–Productivity Tradeoff in Task Switching

Concept. Cognitive Load–Productivity Tradeoff in Task Switching manages analyst workload through prioritization, checklists, rest boundaries, and explicit handoff—not heroics.

Why it matters. Without explicit treatment of **Cognitive Load–Productivity Tradeoff**, heroic overtime undermines workload-aware operator decision hygiene review; the lesson builds the habit to separate cognitive hygiene from heroics, and workload signals from unreviewed urgency.

Source support. Cognitive Load–Productivity Tradeoff in Task Switching rests on [207, 2026]. Its anchor reference records: A 2023 research article in the Proceedings of the Human Factors and Ergonomics Society Annual Meeting by Maximillian Chis and colleagues examining task switching during team-based search-and-rescue scenarios in Minecraft. Use it for the claim that **Cognitive Load–Productivity Tradeoff in Task Switching** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of the Director of National Intelligence, 2015]; [Jr., 2007].

Evidence to inspect. For **Cognitive Load–Productivity Tradeoff**, work from the cited evidence behind this row. [207, 2026] A 2023 research article in the Proceedings of the Human Factors and Ergonomics Society Annual Meeting by Maximillian Chis and colleagues examining task switching during team-based search-and-rescue scenarios in Minecraft. Using an ACT-R model of working memory, the study found that teams switching between task sets less frequently showed both higher cognitive load and higher performance scores. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Cognitive Load–Productivity Tradeoff**, build a **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** for this workload-aware operator decision hygiene topic. The artifact must note the workload descriptor, the bounded claim about **Cognitive Load Productivity Tradeoff in**, the fatigue caveat, the uncertainty margin, the do-not-escalate boundary, and the reviewer who owns the handoff. Shape **Cognitive Load–Productivity Tradeoff** work as a **workload and decision-hygiene card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Cognitive Load–Productivity Tradeoff**: that feeling certain in the moment substitutes for the checklist, pause, and second-look that decision hygiene exists to enforce.

Transfer task. Reuse the **Cognitive Load–Productivity Tradeoff** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

60.2.2.16 Lesson 16: NASA-TLX and Analyst Workload Monitoring

Concept. NASA-TLX and Analyst Workload Monitoring uses workload indexes as review triggers for prioritization, handoff, and rest—not as heroics metrics.

Why it matters. Analysts use **NASA-TLX and Analyst Workload Monitoring** to separate cognitive hygiene from heroics, and workload signals from unreviewed urgency. A defensible treatment names the judgment it enables for workload-aware operator decision hygiene review, the proof limit that heroic overtime would otherwise hide, and the reviewer accountable for challenge.

Source support. NASA-TLX and Analyst Workload Monitoring rests on [179, 2026]. Its anchor reference records: Reviewing 125 articles published between 1998 and 2024, it identifies 129 distinct metrics grouped into non-biometric methods (questionnaires such as NASA-TLX, task performance, interaction tracking) and biometric methods (eye tracking, heart rate). Use it for the claim that **NASA-TLX and Analyst Workload Monitoring** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of the Director of National Intelligence, 2015]; [Jr., 2007].

Evidence to inspect. Read **NASA-TLX and Analyst Workload Monitoring** against the works cited for this row. [179, 2026] An NCSU Laboratory for Analytic Sciences article summarizing a systematic survey of metrics for measuring cognitive load in intelligence-analysis and similar settings. Reviewing 125 articles published between 1998 and 2024, it identifies 129 distinct metrics grouped into non-biometric methods (questionnaires such as NASA-TLX, task performance, interaction tracking) and biometric methods (eye tracking, heart rate). Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. Build a **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** for this workload-aware operator decision hygiene topic. The artifact must note the workload descriptor, the bounded claim about **NASA-TLX and Analyst Workload Monitoring**, the fatigue caveat, the uncertainty margin, the do-not-escalate boundary, and the reviewer who owns the handoff. Shape this subject work as a **workload and decision-hygiene card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **NASA-TLX and Analyst Workload Monitoring**: that feeling certain in the moment substitutes for the checklist, pause, and second-look that decision hygiene exists to enforce.

Transfer task. Reuse the **NASA-TLX and Analyst Workload Monitoring** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

60.2.2.17 Lesson 17: Biometric Monitoring for Real-Time Load Detection

Concept. Biometric Monitoring for Real-Time Load Detection evaluates biometric monitoring by consent, minimization, purpose limits, and human review of alerts.

Why it matters. Biometric Monitoring matters in the **Operator Productivity and Cognitive Performance** lane because workload-aware operator decision hygiene evidence must stay separate from judgment; heroic overtime is a common failure.

Source support. Biometric Monitoring for Real-Time Load Detection rests on [179, 2026]. The closest source to this row notes: Reviewing 125 articles published between 1998 and 2024, it identifies 129 distinct metrics grouped into non-biometric methods (questionnaires such as NASA-TLX, task performance, interaction tracking) and biometric methods (eye tracking, heart rate). Use it for pinning down the scope of **Biometric Monitoring for Real-Time Load Detection**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of the Director of National Intelligence, 2015]; [Jr., 2007].

Evidence to inspect. For **Biometric Monitoring**, reason from the sources cited in this row. [179, 2026] An NCSU Laboratory for Analytic Sciences article summarizing a systematic survey of metrics for measuring cognitive load in intelligence-analysis and similar settings. Reviewing 125 articles published between 1998 and 2024, it identifies 129 distinct metrics grouped into non-biometric methods (questionnaires such as NASA-TLX, task performance, interaction tracking) and biometric methods (eye tracking, heart rate). Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Biometric Monitoring**, build a **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** for this workload-aware operator decision hygiene topic. The artifact must note the workload descriptor, the bounded claim about **Biometric Monitoring for Real-Time Load**, the fatigue caveat, the uncertainty margin, the do-not-escalate boundary, and the reviewer who owns the handoff. Shape **Biometric Monitoring** work as a **workload and decision-hygiene card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Biometric Monitoring**: that feeling certain in the moment substitutes for the checklist, pause, and second-look that decision hygiene exists to enforce.

Transfer task. Reuse the **Biometric Monitoring** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

60.2.2.18 Lesson 18: Spycraft psychology literacy: stress, trust, and reviewer-boundary

Concept. Spycraft psychology literacy: stress, trust, and reviewer-boundary manages workload and bias through prioritization, explicit handoffs, and review checkpoints—not unsustainable pace.

Why it matters. Spycraft psychology literacy connects classroom vocabulary to Operator Productivity and Cognitive Performance practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Spycraft psychology literacy: stress, trust, and reviewer-boundary rests on [025, 2026]. Its anchor reference records: The conversation covers his background at the Air Force Academy and CIA training, and frames espionage as resting on reading people, trust, influence, and empathy rather than glamour or action. Use it for the claim that **Spycraft psychology literacy: stress, trust, and reviewer-boundary** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of the Director of National Intelligence, 2015]; [Jr., 2007].

Evidence to inspect. Read **Spycraft psychology literacy** against the works cited for this row. [025, 2026] This is an episode of The Unmistakable Creative Podcast featuring former CIA field operative Andrew Bustamante discussing intelligence work. The conversation covers his background at the Air Force Academy and CIA training, and frames espionage as resting on reading people, trust, influence, and empathy rather than glamour or action. It also addresses how operatives are selected, the isolation of covert work, and its psychological effects on personal relationships. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Spycraft psychology literacy**, build a **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** for this workload-aware operator decision hygiene topic. The artifact must note the workload descriptor, the bounded claim about **Spycraft psychology literacy**, the fatigue caveat, the uncertainty margin, the do-not-escalate boundary, and the reviewer who owns the handoff. Shape **Spycraft psychology literacy** work as a **workload and decision-hygiene card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Spycraft psychology literacy**: that feeling certain in the moment substitutes for the checklist, pause, and second-look that decision hygiene exists to enforce.

Transfer task. Reuse the **Spycraft psychology literacy** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

60.2.2.19 Lesson 19: MICE motivation literacy and ethical-boundary review for operator psychology

Concept. MICE motivation literacy and ethical-boundary review for operator psychology uses the motivation taxonomy to recognize recruitment-risk narratives and ethics constraints, not to design persuasion.

Why it matters. MICE motivation literacy matters in the **Operator Productivity and Cognitive Performance** lane because workload-aware operator decision hygiene evidence must stay separate from judgment; heroic overtime is a common failure.

Source support. MICE motivation literacy and ethical-boundary review for operator psychology rests on [025, 2026]. The lead source's own note reads: The conversation covers his background at the Air Force Academy and CIA training, and frames espionage as resting on reading

people, trust, influence, and empathy rather than glamour or action. Use it for pinning down the scope of **MICE motivation literacy and ethical-boundary review for operator psychology**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of the Director of National Intelligence, 2015]; [Jr., 2007].

Evidence to inspect. For **MICE motivation literacy**, work from the cited evidence behind this row. [025, 2026] This is an episode of The Unmistakable Creative Podcast featuring former CIA field operative Andrew Bustamante discussing intelligence work. The conversation covers his background at the Air Force Academy and CIA training, and frames espionage as resting on reading people, trust, influence, and empathy rather than glamour or action. It also addresses how operatives are selected, the isolation of covert work, and its psychological effects on personal relationships. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **MICE motivation literacy**, build a **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** for this workload-aware operator decision hygiene topic. The artifact must note the workload descriptor, the bounded claim about **MICE motivation literacy and ethical-boundary**, the fatigue caveat, the uncertainty margin, the do-not-escalate boundary, and the reviewer who owns the handoff. Shape **MICE motivation literacy** work as a **workload and decision-hygiene card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **MICE motivation literacy**: that a motivation taxonomy is a recruitment checklist.

Transfer task. Apply this module's safe boundary for **MICE motivation literacy** to another artifact while keeping workload-aware operator decision hygiene and reviewer ownership explicit.

60.2.2.20 Lesson 20: Trust, Loneliness, and the Psychological Cost of Tradecraft Concept. Trust, Loneliness, and the Psychological Cost of Tradecraft manages workload and bias through prioritization, explicit handoffs, and review checkpoints—not unsustainable pace.

Why it matters. Trust, Loneliness, and the Psychological Cost of Tradecraft matters in the **Operator Productivity and Cognitive Performance** lane because workload-aware operator decision hygiene evidence must stay separate from judgment; heroic overtime is a common failure.

Source support. Trust, Loneliness, and the Psychological Cost of Tradecraft rests on [025, 2026]. The lead source's own note reads: The conversation covers his background at the Air Force Academy and CIA training, and frames espionage as resting on reading people, trust, influence, and empathy rather than glamour or action. Use it for fixing what **Trust, Loneliness, and the Psychological Cost of Tradecraft** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of the Director of National Intelligence, 2015]; [Jr., 2007].

Evidence to inspect. For **Trust, Loneliness, and the Psychological Cost of Tradecraft**, reason from the sources cited in this row. [025, 2026] This is an episode of The Unmistakable Creative Podcast featuring former CIA field operative Andrew Bustamante discussing intelligence work. The conversation covers his background at the Air Force Academy and CIA training, and frames espionage as resting on reading people, trust, influence, and empathy rather than glamour or action. It also addresses how operatives are selected, the isolation of covert work, and its psychological effects on personal relationships. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Trust, Loneliness, and the Psychological Cost of Tradecraft**, build a **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** for this workload-aware operator decision hygiene topic. The artifact must note the workload descriptor, the bounded claim about **Trust Loneliness and the Psychological**, the fatigue caveat, the uncertainty margin, the do-not-escalate boundary, and the reviewer who owns the handoff. Shape this subject work as a **workload and decision-hygiene card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Trust, Loneliness, and the Psychological Cost of Tradecraft**: that feeling certain in the moment substitutes for the checklist, pause, and second-look that decision hygiene exists to enforce.

Transfer task. Reuse the **Trust, Loneliness, and the Psychological Cost of Tradecraft** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

60.2.2.21 Lesson 21: Pattern Recognition, Not Task Management: Operative Cognitive Design Concept. Pattern Recognition, Not Task Management: Operative Cognitive Design uses pattern names as architectural vocabulary for allowlisted, logged, revocable workflows—not as operational playbooks.

Why it matters. Pattern Recognition, Not Task Management connects classroom vocabulary to Operator Productivity and Cognitive Performance practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Pattern Recognition, Not Task Management: Operative Cognitive Design rests on [025, 2026]. Its anchor reference records: It also addresses how operatives are selected, the isolation of covert work, and its psychological effects on personal relationships. Use it for the working definition that **Pattern Recognition, Not Task Management: Operative Cognitive Design** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of the Director of National Intelligence, 2015]; [Jr., 2007].

Evidence to inspect. For **Pattern Recognition, Not Task Management**, reason from the sources cited in this row. [025, 2026] This is an episode of The Unmistakable Creative Podcast featuring former CIA field operative Andrew Bustamante discussing intelligence work. The conversation covers his background at the Air Force Academy and CIA training, and frames espionage as resting on reading people, trust, influence, and empathy rather than glamour or action. It also addresses how operatives are selected, the isolation of covert work, and its psychological effects on personal relationships. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Pattern Recognition, Not Task Management**, build a **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** for this workload-aware operator decision hygiene topic. The artifact must note the workload descriptor, the bounded claim about **Pattern Recognition Task Management**, the fatigue caveat, the uncertainty margin, the do-not-escalate boundary, and the reviewer who owns the handoff. Shape **Pattern Recognition, Not Task Management** work as a **workload and decision-hygiene card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Pattern Recognition, Not Task Management**: that feeling certain in the moment substitutes for the checklist, pause, and second-look that decision hygiene exists to enforce.

Transfer task. Transfer **Pattern Recognition, Not Task Management** from this module to a second motif by preserving workload-aware operator decision hygiene, replacing action with audit, and naming the blocked use.

60.2.2.22 Lesson 22: Circadian Intelligence: Timing Operations to Peak Cognitive Windows Concept. Circadian Intelligence: Timing Operations to Peak Cognitive Windows connects circadian timing to scheduling, rest boundaries, and error-risk review—not operational timing advice.

Why it matters. Circadian Intelligence matters in the **Operator Productivity and Cognitive Performance** lane because workload-aware operator decision hygiene evidence must stay separate from judgment; heroic overtime is a common failure.

Source support. Circadian Intelligence: Timing Operations to Peak Cognitive Windows rests on [308, 2026] and [311, 2026]. Its anchor reference records: It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering. Use them for the working definition that **Circadian Intelligence: Timing Operations to**

Peak Cognitive Windows can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of the Director of National Intelligence, 2015]; [Jr., 2007].

Evidence to inspect. For **Circadian Intelligence**, reason from the sources cited in this row. [308, 2026] An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure. [311, 2026] An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Circadian Intelligence**, build a **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** for this workload-aware operator decision hygiene topic. The artifact must note the workload descriptor, the bounded claim about **Circadian Intelligence**, the fatigue caveat, the uncertainty margin, the do-not-escalate boundary, and the reviewer who owns the handoff. Shape **Circadian Intelligence** work as a **workload and decision-hygiene card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Circadian Intelligence**: that feeling certain in the moment substitutes for the checklist, pause, and second-look that decision hygiene exists to enforce.

Transfer task. Apply this module's safe boundary for **Circadian Intelligence** to another artifact while keeping workload-aware operator decision hygiene and reviewer ownership explicit.

60.2.2.23 Lesson 23: Psychological inoculation and prebunking literacy

Concept. Psychological inoculation and prebunking literacy uses inoculation methods as evidence-informed, bounded, and context-dependent resilience education with transparent labels, source checks, non-manipulative corrections, and explicit measurement limits.

Why it matters. Without explicit treatment of **Psychological inoculation**, treating resilience labels as permission to skip provenance review undermines workload-aware operator decision hygiene review; the lesson builds the habit to separate cognitive hygiene from heroics, and workload signals from unreviewed urgency.

Source support. Psychological inoculation and prebunking literacy rests on [300, 2026], [304, 2026], and [306, 2026]. The closest source to this row notes: NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Use them for pinning down the scope of **Psychological inoculation and prebunking literacy**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of the Director of National Intelligence, 2015]; [Jr., 2007].

Evidence to inspect. Read **Psychological inoculation** against the works cited for this row. [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. Build a **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** for this workload-aware operator decision hygiene topic. The artifact must record the narrative provenance, the bounded claim about **Psychological inoculation**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape this subject work as a **workload and decision-hygiene card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Psychological inoculation**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Apply this module's safe boundary for **Psychological inoculation** to another artifact while keeping workload-aware operator decision hygiene and reviewer ownership explicit.

60.2.2.24 Lesson 24: The Red Zone: How Trauma, PTSD, and Moral Injury Affect Operator Cognition

Concept. The Red Zone: How Trauma, PTSD, and Moral Injury Affect Operator Cognition manages analyst workload through prioritization, checklists, rest boundaries, and explicit handoff—not heroics.

Why it matters. The Red Zone: How Trauma, PTSD, and Moral Injury Affect Operator Cognition matters in the **Operator Productivity and Cognitive Performance** lane because workload-aware operator decision hygiene evidence must stay separate from judgment; heroic overtime is a common failure.

Source support. The Red Zone: How Trauma, PTSD, and Moral Injury Affect Operator Cognition rests on [205, 2026]. The most specific cited work observes: This is the website of the Flow Research Collective, a research and development organization founded in 2018 that studies the neuroscience of human performance and brain health. Use it for the claim that **The Red Zone: How Trauma, PTSD, and Moral Injury Affect Operator Cognition** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of the Director of National Intelligence, 2015]; [Jr., 2007].

Evidence to inspect. Ground **The Red Zone: How Trauma, PTSD, and Moral Injury Affect Operator Cognition** in the evidence the row cites. [205, 2026] This is the website of the Flow Research Collective, a research and development organization founded in 2018 that studies the neuroscience of human performance and brain health. It investigates flow states of focused absorption and applies that research to peak performance training for organizations as well as to mental health conditions such as PTSD and depression. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **The Red Zone**, build a **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** for this workload-aware operator decision hygiene topic. The artifact must note the workload descriptor, the bounded claim about **Red Zone**, the fatigue caveat, the uncertainty margin, the do-not-escalate boundary, and the reviewer who owns the handoff. Shape **The Red Zone: How Trauma, PTSD, and Moral Injury Affect Operator Cognition** work as a **workload and decision-hygiene card** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **The Red Zone: How Trauma, PTSD, and Moral Injury Affect Operator Cognition**: that feeling certain in the moment substitutes for the checklist, pause, and second-look that decision hygiene exists to enforce.

Transfer task. Apply this module's safe boundary for **The Red Zone: How Trauma, PTSD, and Moral Injury Affect Operator Cognition** to another artifact while keeping workload-aware operator decision hygiene and reviewer ownership explicit.

60.2.3 The Intelligent Operator as Cognitive Athlete worked safe example: synthetic inputs, evidence, and review

Worked example: a synthetic analyst cell rebuilds a weekly reading queue after workload scores spike during a surge brief. [262, 2026]; [263, 2026].

Triangulation anchors. In module 43's worked-example section, directly verified anchors for the **Operator Productivity and Cognitive Performance** lane include [of the Director of National Intelligence, 2015]; [Jr., 2007]; [of Standards and Technology, 2022c]. Use them to test source-guide

claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **analyst cognitive performance**. Learners use a **workload and decision-hygiene card** and keep this boundary visible: No productivity optimization may override safety, review, accessibility, rest, or records duties.

Frame. The classroom question centers on **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations**. Excluded actions stay explicit, and the **Operator-Workload Hygiene Lens** planning question is: Which workload signal, capture habit, focus block, and reviewer handoff must stay explicit before the operator accepts more tasking?

Inputs. For the **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations** scenario, use synthetic task lists, NASA-TLX self-ratings, instructor-provided focus blocks, and a handoff template. The Operator-Workload Hygiene Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations**, students capture open loops, score workload, schedule focus blocks, document handoffs, and assign reviewer checkpoints. Pause whenever an inference about Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations** classroom scenario; unit artifact = workload and decision-hygiene card; evidence = allowed inputs; method = workload-aware operator decision hygiene; output = an operator workload card with queue state, TLX scores, focus plan, handoff owner, and rest boundary; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations** as "Operator-Workload Hygiene Lens confirms it" is not enough. The revision ties the claim to workload-aware operator decision hygiene, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

60.2.4 The Intelligent Operator as Cognitive Athlete practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Operator-Workload Hygiene Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations**.

Triangulation anchors. In module 43's practice-sequence section, directly verified anchors for the **Operator Productivity and Cognitive Performance** lane include [of the Director of National Intelligence, 2015]; [Jr., 2007]; [of Standards and Technology, 2022c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations, The Science Behind Getting Things Done: Cognitive Foundations, GTD as External Memory and Affordance System; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Operator Productivity and Cognitive Performance** lane.
2. Frame	Answer the lens question: Which workload signal, capture habit, focus block, and reviewer handoff must stay explicit before the operator accepts more tasking?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations: operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the workload and decision-hygiene card fields for Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations.	Unit profile note.	Evidence artifacts include workload signal, focus-block plan.
4. Challenge	Test the misconception that feeling certain in the moment substitutes for the checklist, pause, and second-look that decision hygiene exists to enforce.	Failure-mode note.	The artifact applies the key distinction: separate cognitive hygiene from heroics, and workload signals from unreviewed urgency.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

60.2.4.1 The Intelligent Operator as Cognitive Athlete instructor notes: source reasoning, review points, and studio focus

Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations**. [262, 2026]; [263, 2026].

60.2.4.2 The Intelligent Operator as Cognitive Athlete extension exercise: peer validation and refresh trigger review

Evidence anchor. Section 60; [262, 2026].

Have learners swap artifacts and apply the **Operator-Workload Hygiene Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations**.

60.2.5 The Intelligent Operator as Cognitive Athlete knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 60; [262, 2026].

1. Explain how **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations** is defined here; name the source descriptor that supports the definition.
2. Contrast **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations** with **The Science Behind Getting Things Done: Cognitive Foundations** using the **Operator-Workload Hygiene Lens** artifact fields.
3. Identify one failure mode from the **Operator Productivity and Cognitive Performance** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which workload signal or handoff gap would have prevented the quality drop?
5. Correct this misconception: that feeling certain in the moment substitutes for the checklist, pause, and second-look that decision hygiene exists to enforce.

60.2.5.1 The Intelligent Operator as Cognitive Athlete answer quality rubric: source evidence, uncertainty, and safe transfer

Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations** without source evidence, uncertainty, or a safe transfer task.

60.3 The Intelligent Operator as Cognitive Athlete assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 60; [262, 2026].

60.3.1 The Intelligent Operator as Cognitive Athlete evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 60; [262, 2026].

60.3.2 The Intelligent Operator as Cognitive Athlete transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 60; [262, 2026].

60.3.2.1 The Intelligent Operator as Cognitive Athlete lineage and source tradition: profile, concepts, and first anchors This sits in the **Operator Productivity and Cognitive Performance** lineage: sustained intelligence work as cognitive performance engineering: external memory, workload measurement, flow conditions, and decision hygiene under operational tempo. [262, 2026]; [263, 2026].

60.3.2.2 The Intelligent Operator as Cognitive Athlete working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 60; [262, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations**, with provenance and reviewability throughout.

60.3.2.3 The Intelligent Operator as Cognitive Athlete knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** source materials, domain constraints, learner questions, verified anchors, and artifact requirements. [262, 2026]; [263, 2026].
- **Transforms:** evidence normalization, structured reasoning, source evaluation, governance review, and handoff preparation.
- **Outputs:** annotated map, decision memo, rubric, tabletop packet, or audit artifact.
- **Failure modes:** over-automation, misplaced confidence, policy drift, and confusing simulation with deployment.

60.3.2.4 The Intelligent Operator as Cognitive Athlete transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 60; [262, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations**.
- **Evidence contract:** keep the **Operator Productivity and Cognitive Performance** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as annotated map, decision memo, rubric, tabletop packet, or audit artifact that another reviewer can audit.

60.3.2.5 The Intelligent Operator as Cognitive Athlete profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 60; [262, 2026].

The matched profile emphasizes sustained intelligence work as cognitive performance engineering: external memory, workload measurement, flow conditions, and decision hygiene under operational tempo. The method stack is GTD capture-clarify-organize cycles, NASA-TLX workload review, flow precondition checklists, task-switching audits, and reviewer handoff under fatigue; the local topic cluster is **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations**.

60.3.3 The Intelligent Operator as Cognitive Athlete evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 60; [262, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Operator Productivity and Cognitive Performance** profile tells reviewers what evidence is strong enough for the module artifact built around **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations**.

60.3.3.1 The Intelligent Operator as Cognitive Athlete guide source spine: inherited keys and local citation roles Primary guide citations: [262, 2026]; [263, 2026]; [264, 2026]; [278, 2026]; [279, 2026]; [283, 2026]; [290, 2026]; [291, 2026]; [294, 2026]; [197, 2026]; [198, 2026]; [199, 2026]; [179, 2026]; [200, 2026]; [201, 2026]; [202, 2026]; [203, 2026]; [204, 2026]; [205, 2026]; [206, 2026]; [207, 2026]; [025, 2026]; [297, 2026]; [298, 2026]; [308, 2026]; [311, 2026]; [300, 2026]; [304, 2026]; [306, 2026].

60.3.3.2 The Intelligent Operator as Cognitive Athlete verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [262, 2026]; [263, 2026].

Tier	What counts	How it is used
Source guide	[262, 2026]; [263, 2026]; [264, 2026]; [278, 2026]; [279, 2026]; [283, 2026]; [290, 2026]; [291, 2026]; [294, 2026]; [197, 2026]; [198, 2026]; [199, 2026]; [179, 2026]; [200, 2026]; [201, 2026]; [202, 2026]; [203, 2026]; [204, 2026]; [205, 2026]; [206, 2026]; [207, 2026]; [025, 2026]; [297, 2026]; [298, 2026]; [308, 2026]; [311, 2026]; [300, 2026]; [304, 2026]; [306, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 43's source-canon section, directly verified anchors for the **Operator Productivity and Cognitive Performance** lane include [of the Director of National Intelligence, 2015]; [Jr., 2007]; [of Standards and Technology, 2022c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations** and [262, 2026]; [263, 2026], but only directly verified source URLs are encoded as citations.

60.3.3.3 The Intelligent Operator as Cognitive Athlete intelligence practice lens: evidence artifact and safety check Practice lens: **Operator-Workload Hygiene Lens** for **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations**. [262, 2026]; [263, 2026].

Planning question: Which workload signal, capture habit, focus block, and reviewer handoff must stay explicit before the operator accepts more tasking?

Evidence artifact: operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary.

Validation rule: separate urgency from authority, workload from quality, and personal tempo claims from measured task-switching cost. Applied to **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations**.

Handoff contract: handoff preserves open loops, TLX scores, evidence packets, reviewer ownership, and blocked-use notes for the next shift.

Safety check: exclude live operational tempo mandates, surveillance of people, performance coercion, and unreviewed tasking under fatigue.

60.3.3.4 The Intelligent Operator as Cognitive Athlete runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 60; [262, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	43.99	43.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind The Intelligent Operator as Cognitive Athlete to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Bounded autonomy, procurement, incident-response, and assurance studio	43.101	43.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for The Intelligent Operator as Cognitive Athlete	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Model-card, recoverability, retention, and learner-support evidence package	43.102	43.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for The Intelligent Operator as Cognitive Athlete	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations	43.1	43.1 Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
The Science Behind Getting Things Done (GTD): Cognitive Foundations	43.2	43.2 The Science Behind Getting Things Done (GTD): Cognitive Foundations	Operator-Workload Hygiene Lens	operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary	exclude live operational tempo mandates, surveillance of people, performance coercion, and unreviewed tasking under fatigue
GTD as External Memory and Affordance System	43.2.1	43.2.1 GTD as External Memory and Affordance System	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
The Five GTD Phases: Capture, Clarify, Organize, Reflect, Engage	43.2.2	43.2.2 The Five GTD Phases: Capture, Clarify, Organize, Reflect, Engage	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Why GTD Improves Team Intelligence Performance (Allen, 2024)	43.2.3	43.2.3 Why GTD Improves Team Intelligence Performance (Allen, 2024)	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
GTD and Reduction of Cognitive Load: Empirical Evidence	43.2.4	43.2.4 GTD and Reduction of Cognitive Load: Empirical Evidence	Operator-Workload Hygiene Lens	operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary	exclude live operational tempo mandates, surveillance of people, performance coercion, and unreviewed tasking under fatigue
Flow State and Peak Performance in Intelligence Work	43.3	43.3 Flow State and Peak Performance in Intelligence Work	Operator-Workload Hygiene Lens	operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary	exclude live operational tempo mandates, surveillance of people, performance coercion, and unreviewed tasking under fatigue
Csikszentmihalyi's Flow: Definition, Seven Conditions, Neurophysiology	43.3.1	43.3.1 Csikszentmihalyi's Flow: Definition, Seven Conditions, Neurophysiology	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Neuroscience of Flow: Prefrontal Cortex Deactivation, Dopamine	43.3.2	43.3.2 Neuroscience of Flow: Prefrontal Cortex Deactivation, Dopamine	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Flow Research Collective	43.3.3	43.3.3 source title transformed into safe curriculum treatment; original: Flow Research Collective	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Go With the Flow: Neuroscientific View on Full Engagement (PMC, 2020)	43.3.4	43.3.4 Go With the Flow: Neuroscientific View on Full Engagement (PMC, 2020)	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Investigating the Flow Experience: Key Conceptual Issues (PMC, 2020)	43.3.5	43.3.5 Investigating the Flow Experience: Key Conceptual Issues (PMC, 2020)	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Engineering Flow State for Intelligence Analysis Environments	43.3.6	43.3.6 Engineering Flow State for Intelligence Analysis Environments	Operator-Workload Hygiene Lens	operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary	exclude live operational tempo mandates, surveillance of people, performance coercion, and unreviewed tasking under fatigue
Cognitive Load Management in Intelligence Work	43.4	43.4 Cognitive Load Management in Intelligence Work	Operator-Workload Hygiene Lens	operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary	exclude live operational tempo mandates, surveillance of people, performance coercion, and unreviewed tasking under fatigue
Cognitive Load–Productivity Tradeoff in Task Switching	43.4.1	43.4.1 Cognitive Load–Productivity Tradeoff in Task Switching	Operator-Workload Hygiene Lens	operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary	exclude live operational tempo mandates, surveillance of people, performance coercion, and unreviewed tasking under fatigue
NASA-TLX and Analyst Workload Monitoring	43.4.2	43.4.2 NASA-TLX and Analyst Workload Monitoring	Operator-Workload Hygiene Lens	operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary	exclude live operational tempo mandates, surveillance of people, performance coercion, and unreviewed tasking under fatigue
Biometric Monitoring for Real-Time Load Detection	43.4.3	43.4.3 Biometric Monitoring for Real-Time Load Detection	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Spycraft psychology literacy: stress, trust, and reviewer-boundary	43.5	43.5 source title transformed into safe curriculum treatment; original: Spycraft and Cognitive Performance: Inside the Operative's Mind	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
MICE motivation literacy and ethical-boundary review for operator psychology	43.5.1	43.5.1 source title transformed into safe curriculum treatment; original: MICE Framework and Moral Flexibility: Operative Psychology	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Trust, Loneliness, and the Psychological Cost of Tradecraft	43.5.2	43.5.2 Trust, Loneliness, and the Psychological Cost of Tradecraft	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Pattern Recognition, Not Task Management: Operative Cognitive Design	43.5.3	43.5.3 Pattern Recognition, Not Task Management: Operative Cognitive Design	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Circadian Intelligence: Timing Operations to Peak Cognitive Windows	43.6	43.6 Circadian Intelligence: Timing Operations to Peak Cognitive Windows	Operator-Workload Hygiene Lens	operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary	exclude live operational tempo mandates, surveillance of people, performance coercion, and unreviewed tasking under fatigue
Psychological inoculation and prebunking literacy	43.7	43.7 source title transformed into safe curriculum treatment; original: Adversarial Stress Inoculation: Preparing the Analyst for High-Stakes Environments	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
The Red Zone: How Trauma, PTSD, and Moral Injury Affect Operator Cognition	43.8	43.8 The Red Zone: How Trauma, PTSD, and Moral Injury Affect Operator Cognition	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings

60.3.3.5 The Intelligent Operator as Cognitive Athlete reusable subsection contract: topic rows, artifacts, and safety duties Evidence anchor. Section 60; [262, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
The Science Behind Getting Things Done (GTD): Cognitive Foundations	Operator-Workload Hygiene Lens	operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary	exclude live operational tempo mandates, surveillance of people, performance coercion, and unreviewed tasking under fatigue
GTD as External Memory and Affordance System	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
The Five GTD Phases: Capture, Clarify, Organize, Reflect, Engage	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Why GTD Improves Team Intelligence Performance (Allen, 2024)	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
GTD and Reduction of Cognitive Load: Empirical Evidence	Operator-Workload Hygiene Lens	operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary	exclude live operational tempo mandates, surveillance of people, performance coercion, and unreviewed tasking under fatigue
Flow State and Peak Performance in Intelligence Work	Operator-Workload Hygiene Lens	operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary	exclude live operational tempo mandates, surveillance of people, performance coercion, and unreviewed tasking under fatigue
Csikszentmihalyi's Flow: Definition, Seven Conditions, Neurophysiology	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Neuroscience of Flow: Prefrontal Cortex Deactivation, Dopamine	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings

Lesson topic	Practice lens	Evidence artifact	Safety check
Flow Research Collective	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Go With the Flow: Neuroscientific View on Full Engagement (PMC, 2020)	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Investigating the Flow Experience: Key Conceptual Issues (PMC, 2020)	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Engineering Flow State for Intelligence Analysis Environments	Operator-Workload Hygiene Lens	operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary	exclude live operational tempo mandates, surveillance of people, performance coercion, and unreviewed tasking under fatigue
Cognitive Load Management in Intelligence Work	Operator-Workload Hygiene Lens	operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary	exclude live operational tempo mandates, surveillance of people, performance coercion, and unreviewed tasking under fatigue
Cognitive Load–Productivity Tradeoff in Task Switching	Operator-Workload Hygiene Lens	operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary	exclude live operational tempo mandates, surveillance of people, performance coercion, and unreviewed tasking under fatigue
NASA-TLX and Analyst Workload Monitoring	Operator-Workload Hygiene Lens	operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary	exclude live operational tempo mandates, surveillance of people, performance coercion, and unreviewed tasking under fatigue
Biometric Monitoring for Real-Time Load Detection	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Spycraft psychology literacy: stress, trust, and reviewer-boundary	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
MICE motivation literacy and ethical-boundary review for operator psychology	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Trust, Loneliness, and the Psychological Cost of Tradecraft	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Pattern Recognition, Not Task Management: Operative Cognitive Design	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Circadian Intelligence: Timing Operations to Peak Cognitive Windows	Operator-Workload Hygiene Lens	operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary	exclude live operational tempo mandates, surveillance of people, performance coercion, and unreviewed tasking under fatigue
Psychological inoculation and prebunking literacy	Cognitive-Resilience Lens	narrative-risk map with provenance, uncertainty, audience harms, and response options	exclude manipulation scripts, impersonation, persuasion targeting, and operational influence planning
The Red Zone: How Trauma, PTSD, and Moral Injury Affect Operator Cognition	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings

60.3.3.6 The Intelligent Operator as Cognitive Athlete annotated source ledger: real titles and local contribution Each source cited by this **Operator Productivity and Cognitive Performance** module is paired below with its real title and a one-line note on what it contributes to **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations**.

Source	Cited work	What it contributes	Status
[262, 2026]	Artificial Intelligence	The International Labour Organization's topic portal on artificial intelligence and the world of work. It examines AI's dual role in automating worker tasks and in automating managerial functions through algorithmic management, arguing that whether AI displaces or complements jobs depends on how technology is integrated into work processes.	verified source-guide

Source	Cited work	What it contributes	Status
[263, 2026]	Mind the AI Divide: Shaping a Global Perspective on the Future of Work	A joint UN and International Labour Organization report (July 2024) titled 'Mind the AI Divide,' examining how unequal AI adoption can deepen global inequality. It argues that disparities in digital infrastructure, technology, education, and training risk leaving less developed nations further behind as economies shift toward AI-driven production.	verified source-guide
[264, 2026]	Global Commission on the Future of Work	An International Labour Organization news article (January 2019) announcing the findings of the ILO Global Commission on the Future of Work, a 15-month study co-chaired by the leaders of South Africa and Sweden. The commission issued ten recommendations addressing workplace change driven by technological and demographic shifts, including universal labor protections, lifelong learning, and stronger social safety nets.	verified source-guide
[278, 2026]	Recommendation of the Council on Public Procurement	The OECD Recommendation of the Council on Public Procurement (OECD/LEGAL/0411), a legal instrument adopted by the OECD Council in 2015 on the proposal of the Public Governance Committee. It frames public procurement as a pillar of strategic governance and service delivery and sets out principles for governments to follow.	verified source-guide
[279, 2026]	Open Contracting Data Standard	The documentation homepage for the Open Contracting Data Standard, version 1.1.5, maintained by the Open Contracting Partnership to support disclosure of government contracting data across the procurement lifecycle. It provides a common data model spanning planning, tender, award, contract, and implementation stages, along with a primer, implementation guidance, technical schemas, and validation tooling.	verified source-guide
[283, 2026]	Recommendation of the Council on Open Government	An OECD legal instrument document reproducing the Recommendation of the Council on Open Government (OECD/LEGAL/0438), adopted on 14 December 2017. It defines open government as a culture of governance promoting transparency, integrity, accountability, and stakeholder participation in support of democracy and inclusive growth.	verified source-guide
[290, 2026]	NIST SP 800-218A: Secure Software Development Practices for Generative AI and Dual-Use Foundation Models	NIST Special Publication 800-218A (July 2024), which augments the Secure Software Development Framework with practices specific to AI model development across the software lifecycle. Produced in response to Executive Order 14110, it addresses AI model producers, developers building on those models, and acquirers of AI systems, and is designed to be used alongside NIST SP 800-218.	verified source-guide

Source	Cited work	What it contributes	Status
[291, 2026]	Revised 508 Standards and 255 Guidelines	Official documentation from the U.S. Access Board on the Revised 508 Standards and 255 Guidelines for information and communication technology accessibility. It establishes mandatory accessibility requirements for federal agencies and voluntary guidelines for telecommunications manufacturers, covering hardware, software, websites, electronic documents, and support services.	verified source-guide
[294, 2026]	M-25-21: Accelerating Federal Use of AI through Innovation, Governance, and Public Trust	An April 2025 Office of Management and Budget memorandum (M-25-21) directing executive branch agencies on federal use of artificial intelligence. Issued under Executive Order 14179, it instructs agencies to accelerate adoption of AI to improve public services and government efficiency while maintaining safeguards for civil rights, civil liberties, and privacy.	verified source-guide
[197, 2026]	Getting Things Done: The Science behind Stress-Free Productivity	In 2001 David Allen proposed 'Getting Things Done' (GTD) as a method for enhancing personal.	original source-guide
[198, 2026]	Metoda GTD = Getting Things Done - Lukáš Barda	A Czech-language explainer of the Getting Things Done (GTD) productivity method created by David Allen. It describes the system's core steps of capturing thoughts, clarifying them into actionable items, organizing and prioritizing, regularly reviewing, and executing, including the principle of doing any task that takes under two minutes immediately. The page also surveys software tools for implementing GTD, such as Todoist, OmniFocus, Trello, Evernote, and Notion.	verified source-guide
[199, 2026]	David Allen Explains Why GTD Improves Team Performance	See bibliography for scope.	original source-guide
[179, 2026]	Survey of Metrics for Cognitive Load in Intelligence Community	An NCSU Laboratory for Analytic Sciences article summarizing a systematic survey of metrics for measuring cognitive load in intelligence-analysis and similar settings. Reviewing 125 articles published between 1998 and 2024, it identifies 129 distinct metrics grouped into non-biometric methods (questionnaires such as NASA-TLX, task performance, interaction tracking) and biometric methods (eye tracking, heart rate).	verified source-guide
[200, 2026]	The Science Behind Flow State / Achieving Optimal Performance	A marketing blog post on the Dingbats Notebooks e-commerce site about flow state and how writing tools can support it. It summarizes Mihaly Csikszentmihalyi's concept of flow as a state of full absorption marked by intense focus, clear goals, and immediate feedback, and reviews associated benefits and neuroscience such as reduced prefrontal-cortex activity and increased dopamine.	verified source-guide

Source	Cited work	What it contributes	Status
[201, 2026]	Go with the flow: A neuroscientific view on being fully engaged	A 2020 theoretical review article in the European Journal of Neuroscience by van der Linden, Tops, and Bakker proposing a neuroscientific model of flow, the state of full task absorption with strong drive and low self-referential thinking. The authors argue that the dopamine and norepinephrine systems drive the motivational and mood components of flow, and that interaction among the default mode, central executive, and salience networks produces its characteristic features.	verified source-guide
[202, 2026]	Flow (psychology)	A Wikipedia article on flow, the psychological state of complete immersion and focused engagement in an activity, also known as being in the zone. It traces the concept to psychologist Mihaly Csikszentmihalyi and describes flow as a balance between challenge and skill, characterized by intense concentration, merging of action and awareness, loss of self-consciousness, a sense of control, distorted time perception, and intrinsic reward.	verified source-guide context; do not use as primary analytic support
[203, 2026]	How Flow Theory Unleashes High Performance in Your Career	A blog article applying Mihaly Csikszentmihalyi's Flow Theory to workplace and career performance. It describes flow as a state of full absorption in an activity, lists conditions associated with it such as clear goals, immediate feedback, and a balance between challenge and skill, and discusses how time can appear distorted during flow. The piece argues that achieving flow states enhances productivity and job satisfaction across roles and industries.	verified source-guide
[204, 2026]	The Neuroscience of Flow State: How the Brain Reaches Peak	A LinkedIn article (Sana Noor, 2024) on the neuroscience of flow, the state of complete immersion in a task. It describes brain mechanisms associated with flow, including reduced prefrontal activity (transient hypofrontality) that lowers self-consciousness, dopamine-driven motivation, and deactivation of the default mode network to enable deep focus.	verified practitioner context; secondary evidence only
[205, 2026]	Flow Research Collective: Neuroscience of Human Performance	This is the website of the Flow Research Collective, a research and development organization founded in 2018 that studies the neuroscience of human performance and brain health. It investigates flow states of focused absorption and applies that research to peak performance training for organizations as well as to mental health conditions such as PTSD and depression.	verified source-guide
[206, 2026]	Investigating the "Flow" Experience: Key Conceptual	A 2020 conceptual analysis by Sami Abuhamdeh in Frontiers in Psychology arguing that flow research has stalled because the construct is operationalized inconsistently across studies. It identifies disagreements over whether flow is a discrete state or a continuum, whether enjoyment is essential to it, and whether scales conflate flow's conditions with the experience itself.	verified source-guide

Source	Cited work	What it contributes	Status
[207, 2026]	The Cognitive Load – Productivity Tradeoff in Task Switching	A 2023 research article in the Proceedings of the Human Factors and Ergonomics Society Annual Meeting by Maximillian Chis and colleagues examining task switching during team-based search-and-rescue scenarios in Minecraft. Using an ACT-R model of working memory, the study found that teams switching between task sets less frequently showed both higher cognitive load and higher performance scores.	verified source-guide
[025, 2026]	Andrew Bustamante: Inside the Mind of a Spy — Tradecraft, Trust	This is an episode of The Unmistakable Creative Podcast featuring former CIA field operative Andrew Bustamante discussing intelligence work. The conversation covers his background at the Air Force Academy and CIA training, and frames espionage as resting on reading people, trust, influence, and empathy rather than glamour or action. It also addresses how operatives are selected, the isolation of covert work, and its psychological effects on personal relationships.	verified source-guide
[297, 2026]	Intelligence Community Directive 203: Analytic Standards	Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products.	original source-guide
[298, 2026]	Intelligence Community Directives	Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations.	original source-guide
[308, 2026]	Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure	An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure.	verified source-guide
[311, 2026]	Countering Information Threats	An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering.	verified source-guide
[300, 2026]	MITRE ATLAS	MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy.	original source-guide
[304, 2026]	Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities	NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences.	verified source-guide

Source	Cited work	What it contributes	Status
[306, 2026]	Artificial Intelligence	Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support.	original source-guide

Where this sits. This module's overview is Section 60; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

60.3.4 The Intelligent Operator as Cognitive Athlete governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 60; [262, 2026].

60.3.5 The Intelligent Operator as Cognitive Athlete analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 43's governance-boundary section, directly verified anchors for the **Operator Productivity and Cognitive Performance** lane include [of the Director of National Intelligence, 2015]; [Jr., 2007]; [of Standards and Technology, 2022c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **Operator Productivity and Cognitive Performance** for **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done (GTD): Cognitive Foundations**. [262, 2026]; [263, 2026].

Curriculum topic spine: Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations, **The Science Behind Getting Things Done (GTD): Cognitive Foundations**, **GTD as External Memory and Affordance System**. **Verified anchor cluster:** [of the Director of National Intelligence, 2015]; [Jr., 2007]; [of Standards and Technology, 2022c].

Conceptual depth: sustained intelligence work as cognitive performance engineering: external memory, workload measurement, flow conditions, and decision hygiene under operational tempo.

Method stack: GTD capture-clarify-organize cycles, NASA-TLX workload review, flow precondition checklists, task-switching audits, and reviewer handoff under fatigue.

Composability contract: requirements queues, workload signals, focus blocks, evidence packets, and reviewer checkpoints remain separable artifacts.

Known failure modes: heroic overtime, invisible cognitive debt, context-switch thrash, uncalibrated confidence under load, and skipping handoff review.

Defensive boundary: productivity material stays educational and synthetic; it does not prescribe live operational tempo, surveillance of people, or performance coercion. Applied to **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done (GTD): Cognitive Foundations**.

Anchor	Why it matters here
[of the Director of National Intelligence, 2015]	Official ODNI analytic tradecraft standards directive. Checked as of 2026-05-21; role: source_quality_anchor.
[Jr., 2007]	Foundational analytic cognition source for bias, mental models, and structured reasoning. Checked as of 2026-06-06; role: curriculum_anchor.
[of Standards and Technology, 2022c]	Official supply-chain risk-management guidance for identifying, assessing, and mitigating product, service, vendor, and process risks. Checked as of 2026-05-21; role: curriculum_anchor.

60.3.5.1 The Intelligent Operator as Cognitive Athlete evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **Operator Productivity and Cognitive Performance** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [262, 2026]; [263, 2026].

60.3.6 The Intelligent Operator as Cognitive Athlete agentic boundary: assist, approve, block, and record

Evidence anchor. Section 60; [262, 2026].

AGEINT translation is bounded by the **Operator Productivity and Cognitive Performance** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations**.

60.3.6.1 The Intelligent Operator as Cognitive Athlete permitted defensive utility: curriculum uses and safe outputs **Evidence anchor.** Section 60; [262, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations**.

60.3.6.2 The Intelligent Operator as Cognitive Athlete excluded operational boundary: blocked actions and stop rules Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [262, 2026]; [263, 2026] and **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

60.3.7 The Intelligent Operator as Cognitive Athlete governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 60; [262, 2026].

Governance is practiced as a gate on the **Operator Productivity and Cognitive Performance** lane. Learners use the **Operator-Workload Hygiene Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations**.

60.3.7.1 The Intelligent Operator as Cognitive Athlete governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [262, 2026]; [263, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner

Gate	Coursebook check	Evidence retained
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Operator Productivity and Cognitive Performance** failure modes and the **Operator-Workload Hygiene Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

60.3.7.2 The Intelligent Operator as Cognitive Athlete evidence package handoff: appendices, records, and reuse Evidence anchor. Section 60; [262, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Operator-Workload Hygiene Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations**.

60.3.7.3 The Intelligent Operator as Cognitive Athlete current-source assurance: verified anchors and local artifact fit The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations**. [262, 2026]; [263, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_odni_icd_203` for **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations**?	Intelligence Community Directive 203: Analytic Standards; lane `source_quality_spine`; checked 2026-05-21.	operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary; Official ODNI analytic tradecraft standards directive.
What does the module inherit from `scholarly_heuer_psychology_intelligence_analysis` for **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations**?	Psychology of Intelligence Analysis; lane `analytic_tradecraft`; checked 2026-06-06.	operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary; Foundational analytic cognition source for bias, mental models, and structured reasoning.
What does the module inherit from `official_nist_sp_800_161r1` for **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations**?	Cybersecurity Supply Chain Risk Management Practices, NIST SP 800-161 Rev. 1; lane `cyber_threat_intelligence`; checked 2026-05-21.	operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary; Official supply-chain risk-management guidance for identifying, assessing, and mitigating product, service, vendor, and process risks.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 60; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

60.3.8 The Intelligent Operator as Cognitive Athlete assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 60; [262, 2026].

60.3.9 The Intelligent Operator as Cognitive Athlete assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 60; [262, 2026].

60.3.9.1 The Intelligent Operator as Cognitive Athlete capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations**.
Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations** and [262, 2026]; [263, 2026].

60.3.9.2 The Intelligent Operator as Cognitive Athlete instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations** and [262, 2026]; [263, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

60.3.9.3 The Intelligent Operator as Cognitive Athlete assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations	Completed **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
The Science Behind Getting Things Done (GTD): Cognitive Foundations	Completed **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
GTD as External Memory and Affordance System	Completed **operator workload card with queue state, NASA-TLX ratings, focus plan, handoff owner, and rest boundary** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

60.3.10 The Intelligent Operator as Cognitive Athlete refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [262, 2026]; [263, 2026] and **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations**.

60.3.10.1 The Intelligent Operator as Cognitive Athlete refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations**. The local signals begin with [262, 2026]; [263, 2026].

60.3.10.2 The Intelligent Operator as Cognitive Athlete claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations**, and the source spine for these checks begins with [262, 2026]; [263, 2026].

60.3.11 The Intelligent Operator as Cognitive Athlete reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [262, 2026]; [263, 2026].
Triangulation anchors. In module 43's review-checklist section, directly verified anchors for the **Operator Productivity and Cognitive Performance** lane include [of the Director of National Intelligence, 2015]; [Jr., 2007]; [of Standards and Technology, 2022c]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations**. [262, 2026]; [263, 2026].

- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

60.3.12 The Intelligent Operator as Cognitive Athlete learning-path links: module map, overview, and curriculum atlas

Follow the cross-links to move between **Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations; The Science Behind Getting Things Done: Cognitive Foundations** and the rest of the curriculum without losing the source spine: orientation first, then the parent unit, then the modules on either side. Primary sources: [262, 2026]; [263, 2026].

Section 2, Section 59, Section 61

61 Information Architecture for Intelligence Work

61.0.1 Information Architecture for Intelligence Work figures and course links: visual evidence, source flow, and navigation

The module uses Figure 132, Figure 133, and Figure 129 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 59, Section 60, Section 62.
This module teaches the **Governed Intelligence Cycle and Dissemination Architecture** lane through a bounded, source-backed coursebook chapter. [251, 2026]; [268, 2026].

61.1 Governed Intelligence Cycle and Dissemination Architecture frame for Information Architecture for Intelligence Work: source context, topic focus, and reader task

Evidence anchor. Section 61; [251, 2026].

61.1.1 Information Architecture for Intelligence Work orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 61; [251, 2026].

61.1.2 Information Architecture for Intelligence Work conceptual primer: source context, core model, and reader task

This chapter teaches intelligence as a governed information cycle: requirements become collection, collection becomes evaluated evidence, evidence becomes analytic judgment, and judgment becomes a disseminated product with markings, records, feedback, and oversight. The chapter uses **Dissemination-and-Marking Control Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**.
The central distinction is to separate intelligence work from ordinary research by naming authority, audience, caveats, and feedback. Core topics include **Personal Knowledge Management (PKM) Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers; Obsidian, Roam Research, LogSeq: PKM Tools for Analysts**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Community, 2026]; [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026c]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [251, 2026]; [268, 2026].
Learners move from vocabulary and the **Dissemination-and-Marking Control Lens** distinction through topic lessons on **Personal Knowledge Management (PKM) Systems for Intelligence Professionals** with evidence and misconception checks, then assemble a **dissemination map with audience, caveat, marking, records, and feedback fields** with safety and rights gates.

61.1.3 Information Architecture for Intelligence Work learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 61; [251, 2026].

- Connect **Personal Knowledge Management (PKM) Systems for Intelligence Professionals and Zettelkasten: German Note-Taking System for Researchers** to **Governed Intelligence Cycle and Dissemination Architecture** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **dissemination map with audience, caveat, marking, records, and feedback fields** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate intelligence work from ordinary research by naming authority, audience, caveats, and feedback; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as cycle theater, undocumented dissemination, classification drift, unclear release authority, stale records assumptions, and feedback loops that hide bias, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: cycle and marking material remains public-source and educational; it never handles classified content, live release decisions, or source-method exposure.

61.1.4 Information Architecture for Intelligence Work core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 61; [251, 2026].

Term	Working definition
Requirement	the decision need or learning question that justifies evidence collection
Dissemination	the controlled movement of an intelligence product to an authorized audience
Marking	the vocabulary that communicates handling, caveat, and release limits
Feedback loop	the customer or reviewer signal that tests whether the product answered the need
Records duty	the retention, deletion, or refresh obligation attached to an artifact
Decision hygiene	habits that keep requirements, evidence, and reviewer judgment aligned under load
Information architecture	how sources, notes, and products are organized so uncertainty stays visible
Personal Knowledge Management (PKM) Systems for…	Key terms: Personal, Knowledge, Management.
Zettelkasten: German Note-Taking System for…	Key terms: Zettelkasten, German, Note.

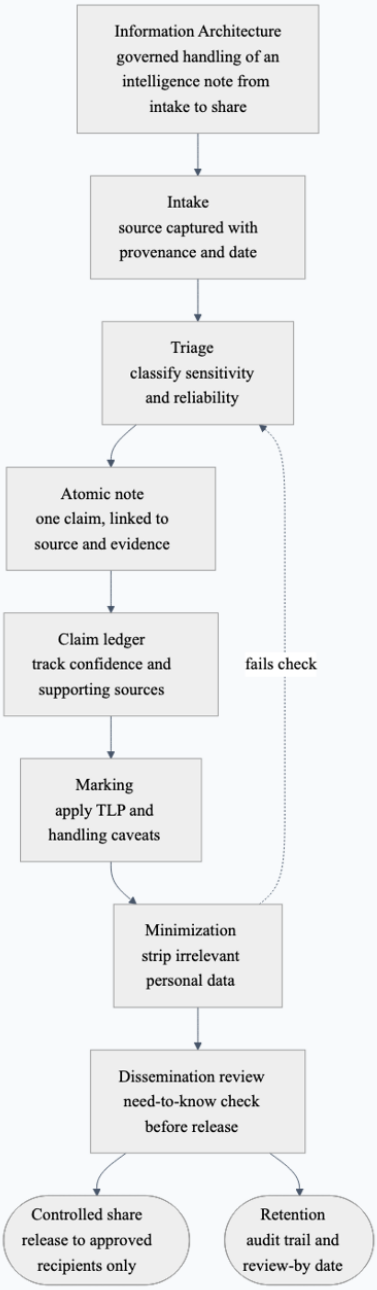


Figure 132: This diagram teaches the disciplined path a single intelligence note travels from intake to controlled sharing, with provenance, a claim ledger, marking, and minimization gating release. It is anchored to the productivity intelligence and cognitive performance / information architecture for intelligence work section; use it to inspect Information Architecture governed handling of an intelligence note from intake to share, Intake source captured with provenance and date, Triage classify sensitivity and reliability, and Atomic note one claim, linked to source and evidence while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

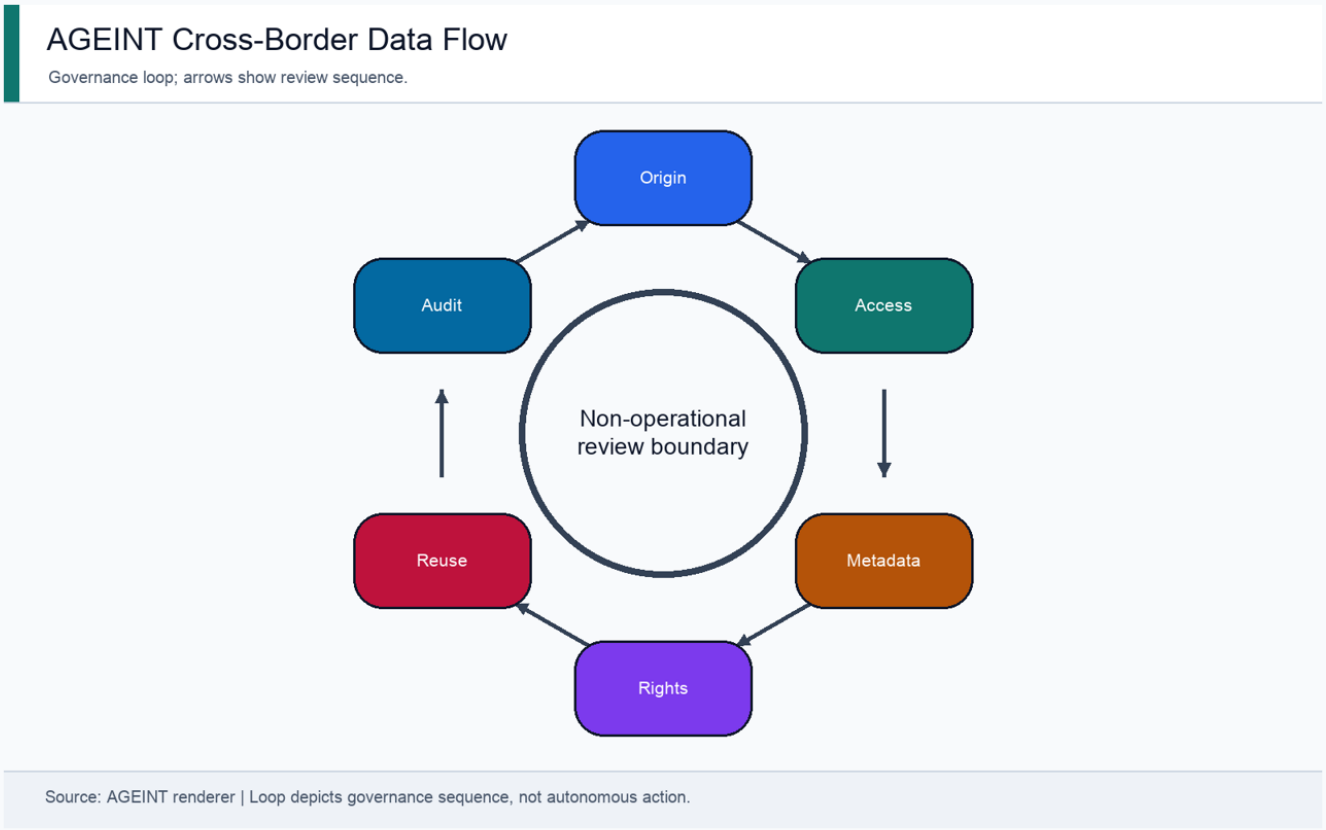


Figure 133: The cross-border data flow shows how access, metadata, rights, and reuse decisions are governed. Its reader value is to make cross border data flow steps, decision gates, owner handoffs, refresh triggers, and closure evidence visible at a glance, with the productivity intelligence and cognitive performance / information architecture for intelligence work section as the source section and defensive review as the boundary.

61.2 Dissemination-and-Marking Control Lens path for Information Architecture for Intelligence Work: lesson cluster, safe artifact, and review

Evidence anchor. Section 61; [251, 2026].

61.2.1 Information Architecture for Intelligence Work practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 61; [251, 2026].

61.2.2 Information Architecture for Intelligence Work topic lessons: source-backed concepts and transfer tasks

This module builds intelligence as a governed information cycle: requirements become collection, collection becomes evaluated evidence, evidence becomes analytic judgment, and judgment becomes a disseminated product with markings, records, feedback, and oversight. The sequence opens with **Personal Knowledge Management (PKM) Systems for Intelligence Professionals**, **Zettelkasten: German Note-Taking System for Researchers**, **Obsidian, Roam Research, LogSeq: PKM Tools for Analysts** and applies the **Dissemination-and-Marking Control Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 129; module overview Section 61; curriculum atlas Section 2.

Triangulation anchors. In module 44's topic-lessons section, directly verified anchors for the **Governed Intelligence Cycle and Dissemination Architecture** lane include [Community, 2026]; [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026c]; [of the Director of National Intelligence, 2025a]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

61.2.2.1 Lesson 1: Personal Knowledge Management (PKM) Systems for Intelligence Professionals

Concept. Personal Knowledge Management (PKM) Systems for Intelligence Professionals designs information flows so requirements, sources, judgments, and records remain discoverable and auditable.

Why it matters. Personal Knowledge Management (PKM) Systems matters in the **Governed Intelligence Cycle and Dissemination Architecture** lane because cycle mapping and audience-aware product design evidence must stay separate from judgment; cycle theater is a common failure.

Source support. Personal Knowledge Management (PKM) Systems for Intelligence Professionals rests on [308, 2026] and [311, 2026]. The most specific cited work observes: It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering. Use them for the working definition that **Personal Knowledge Management (PKM) Systems for Intelligence Professionals** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2015].

Evidence to inspect. Ground **Personal Knowledge Management (PKM) Systems** in the evidence the row cites. [308, 2026] An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure. [311, 2026] An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Personal Knowledge Management (PKM) Systems**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this cycle mapping and audience-aware product design topic. The artifact must name the source descriptor, the bounded claim about **Personal Knowledge Management Systems for**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Personal Knowledge Management (PKM) Systems** work as a **workload and decision-hygiene card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that Personal Knowledge Management (PKM) Systems for Intelligence Professionals replaces human review whenever evidence looks plausible.

Transfer task. Transfer **Personal Knowledge Management (PKM) Systems** to a second module by preserving cycle mapping and audience-aware product design, changing the source evidence, and naming a new reviewer.

61.2.2.2 Lesson 2: Zettelkasten: German Note-Taking System for Researchers

Concept. Zettelkasten: German Note-Taking System for Researchers treats linked notes as provenance-aware evidence cards, not a substitute for source validation or dissemination marking.

Why it matters. Zettelkasten: German Note-Taking System for Researchers connects classroom vocabulary to Governed Intelligence Cycle and Dissemination Architecture practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Zettelkasten: German Note-Taking System for Researchers rests on [307, 2026], [305, 2026], and [304, 2026]. The lead source's own note reads: NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Use them for the claim that **Zettelkasten: German Note-Taking System for Researchers** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2015].

Evidence to inspect. Ground **Zettelkasten: German Note-Taking System for Researchers** in the evidence the row cites. [307, 2026] Official CISA Industrial Control Systems recommended practices page for defensive ICS/OT safety, resilience, and incident-preparation guidance. [305, 2026] Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Zettelkasten**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this cycle mapping and audience-aware product design topic. The artifact must name the source descriptor, the bounded claim about **Zettelkasten**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Zettelkasten: German Note-Taking System for Researchers** work as a **workload and decision-hygiene card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that Zettelkasten: German Note-Taking System for Researchers can be used while ignoring the rule to separate intelligence work from ordinary research by naming authority, audience, caveats, and feedback.

Transfer task. Transfer **Zettelkasten: German Note-Taking System for Researchers** to a second module by preserving cycle mapping and audience-aware product design, changing the source evidence, and naming a new reviewer.

61.2.2.3 Lesson 3: Obsidian, Roam Research, LogSeq: PKM Tools for Analysts

Concept. Obsidian, Roam Research, LogSeq: PKM Tools for Analysts evaluates PKM tools by provenance, access control, exportability, and review gates—not by collection volume.

Why it matters. Obsidian, Roam Research, LogSeq matters in the **Governed Intelligence Cycle and Dissemination Architecture** lane because cycle mapping and audience-aware product design evidence must stay separate from judgment; cycle theater is a common failure.

Source support. Obsidian, Roam Research, LogSeq: PKM Tools for Analysts rests on [052, 2026], [051, 2026], and [269, 2026]. The lead source's own note reads: It offers 35 best practices for publishing and consuming data on the Web, covering metadata, licensing and provenance, data quality, dataset versioning, persistent URIs, machine-readable formats, vocabulary reuse, access methods, preservation, and feedback. Use them for pinning down the scope of **Obsidian, Roam Research, LogSeq: PKM Tools for Analysts**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2015].

Evidence to inspect. Ground **Obsidian, Roam Research, LogSeq** in the evidence the row cites. [052, 2026] This article defines open source intelligence as the practice of gathering information from publicly available data for security, business, and investigative purposes, drawing on websites, social media, government records, and public databases. [269, 2026] A W3C Recommendation, "Data on the Web Best Practices," published January 31, 2017 by the Data on the Web Best Practices Working Group. It offers 35 best practices for publishing and consuming data on the Web, covering metadata, licensing and provenance, data quality, dataset versioning, persistent URIs, machine-readable formats, vocabulary reuse, access methods, preservation, and feedback. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Obsidian, Roam Research, LogSeq**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this cycle mapping and audience-aware product design topic. The artifact must name the source descriptor, the bounded claim about **Obsidian Roam Research LogSeq**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Obsidian, Roam Research, LogSeq** work as a **workload and decision-hygiene card** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that Obsidian, Roam Research, LogSeq: PKM Tools for Analysts is optional whenever separate intelligence work from ordinary research by naming authority, audience, caveats, and feedback feels inconvenient.

Transfer task. Transfer **Obsidian, Roam Research, LogSeq** to a second module by preserving cycle mapping and audience-aware product design, changing the source evidence, and naming a new reviewer.

61.2.2.4 Lesson 4: Second Brain Methodology Applied to Intelligence Collection

Concept. Second Brain Methodology Applied to Intelligence Collection connects cognitive science claims to analytic bias literacy: what the brain prioritizes, what it misses, and how review compensates.

Why it matters. Analysts use **Second Brain Methodology Applied** to separate intelligence work from ordinary research by naming authority, audience, caveats, and feedback. A defensible treatment names the judgment it enables for cycle mapping and audience-aware product design review, the proof limit that cycle theater would otherwise hide, and the reviewer accountable for challenge.

Source support. Second Brain Methodology Applied to Intelligence Collection rests on [308, 2026] and [311, 2026]. The lead source's own note reads: An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. Use them for pinning down the scope of **Second Brain Methodology Applied to Intelligence Collection**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2015].

Evidence to inspect. Read **Second Brain Methodology Applied** against the works cited for this row. [308, 2026] An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure. [311, 2026] An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Second Brain Methodology Applied**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this cycle mapping and audience-aware product design topic. The artifact must name the source descriptor, the bounded claim about **Second Brain Methodology Applied to**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Second Brain Methodology Applied** work as a **workload and decision-hygiene card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that Second Brain Methodology Applied to Intelligence Collection establishes intent without reviewing alternative explanations.

Transfer task. Transfer **Second Brain Methodology Applied** to a second module by preserving cycle mapping and audience-aware product design, changing the source evidence, and naming a new reviewer.

61.2.2.5 Lesson 5: Information Diet and Source Hygiene

Concept. Information Diet and Source Hygiene designs intake boundaries so requirements, sources, and judgments stay separate from noise and unverified feeds.

Why it matters. Without explicit treatment of **Information Diet**, cycle theater undermines cycle mapping and audience-aware product design review; the lesson builds the habit to separate intelligence work from ordinary research by naming authority, audience, caveats, and feedback.

Source support. Information Diet and Source Hygiene rests on [308, 2026] and [311, 2026]. Its anchor reference records: An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. Use them for the working definition that **Information Diet and Source Hygiene** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2015].

Evidence to inspect. Ground **Information Diet** in the evidence the row cites. [308, 2026] An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure. [311, 2026] An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. Build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this cycle mapping and audience-aware product design topic. The artifact must name the source descriptor, the bounded claim about **Information Diet**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape this subject work as a **workload and decision-hygiene card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that Information Diet and Source Hygiene replaces human review whenever evidence looks plausible.

Transfer task. Transfer **Information Diet** to a second module by preserving cycle mapping and audience-aware product design, changing the source evidence, and naming a new reviewer.

61.2.2.6 Lesson 6: Distraction Architecture: Designing Environments for Deep Analytical Work Concept. Distraction Architecture: Designing Environments for Deep Analytical Work designs intake boundaries so requirements, sources, and judgments stay separate from noise and unverified feeds.

Why it matters. Analysts use **Distraction Architecture** to separate intelligence work from ordinary research by naming authority, audience, caveats, and feedback. A defensible treatment names the judgment it enables for cycle mapping and audience-aware product design review, the proof limit that cycle theater would otherwise hide, and the reviewer accountable for challenge.

Source support. Distraction Architecture: Designing Environments for Deep Analytical Work rests on [309, 2026], [310, 2026], and [300, 2026]. The closest source to this row notes: It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). Use them for the claim that **Distraction Architecture: Designing Environments for Deep Analytical Work** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2015].

Evidence to inspect. Ground **Distraction Architecture** in the evidence the row cites. [309, 2026] An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection. [310, 2026] The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe). [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Distraction Architecture**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this cycle mapping and audience-aware product design topic. The artifact must name the source descriptor, the bounded claim about **Distraction Architecture**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Distraction Architecture** work as a **workload and decision-hygiene card** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that Distraction Architecture: Designing Environments for Deep Analytical Work can be used while ignoring the rule to separate intelligence work from ordinary research by naming authority, audience, caveats, and feedback.

Transfer task. Transfer **Distraction Architecture** to a second module by preserving cycle mapping and audience-aware product design, changing the source evidence, and naming a new reviewer.

61.2.2.7 Lesson 7: Collaborative Intelligence: Team Workflows, Shared Notes, Secure Platforms Concept. Collaborative Intelligence: Team Workflows, Shared Notes, Secure Platforms applies Collaborative, Team, Workflows within Governed Intelligence Cycle and Dissemination Architecture: learners use separate intelligence work from ordinary research by naming authority, audience, caveats, and feedback and cycle mapping and audience-aware product design evidence before any judgment moves forward.

Why it matters. Without explicit treatment of **Collaborative Intelligence**, cycle theater undermines cycle mapping and audience-aware product design review; the lesson builds the habit to separate intelligence work from ordinary research by naming authority, audience, caveats, and feedback.

Source support. Collaborative Intelligence: Team Workflows, Shared Notes, Secure Platforms rests on [307, 2026], [305, 2026], and [304, 2026]. Its anchor reference records: NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Use them for the claim that **Collaborative Intelligence: Team Workflows, Shared Notes, Secure Platforms** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2015].

Evidence to inspect. For **Collaborative Intelligence**, work from the cited evidence behind this row. [307, 2026] Official CISA Industrial Control Systems recommended practices page for defensive ICS/OT safety, resilience, and incident-preparation guidance. [305, 2026] Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Collaborative Intelligence**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this cycle mapping and audience-aware product design topic. The artifact must name the source descriptor, the bounded claim about **Collaborative Intelligence**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Collaborative Intelligence** work as a **workload and decision-hygiene card** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that Collaborative Intelligence: Team Workflows, Shared Notes, Secure Platforms is optional whenever separate intelligence work from ordinary research by naming authority, audience, caveats, and feedback feels inconvenient.

Transfer task. Transfer **Collaborative Intelligence** to a second module by preserving cycle mapping and audience-aware product design, changing the source evidence, and naming a new reviewer.

61.2.2.8 Lesson 8: The Analyst's Toolkit: Hardware, Software, and Network Configuration Concept. The Analyst's Toolkit: Hardware, Software, and Network Configuration applies Analyst, Toolkit, Hardware within Governed Intelligence Cycle and Dissemination Architecture: learners use separate intelligence work from ordinary research by naming authority, audience, caveats, and feedback and cycle mapping and audience-aware product design evidence before any judgment moves forward.

Why it matters. The Analyst's Toolkit connects classroom vocabulary to Governed Intelligence Cycle and Dissemination Architecture practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. The Analyst's Toolkit: Hardware, Software, and Network Configuration rests on [055, 2026], [051, 2026], and [301, 2026]. Its anchor reference records: Official Intelligence Community strategy for open-source intelligence governance, integration, source discovery, data, tools, tradecraft, and workforce priorities. Use them for the working definition that **The Analyst's Toolkit: Hardware, Software, and Network Configuration** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Community, 2026]; [of the Director of National Intelligence, 2015].

Evidence to inspect. For **The Analyst's Toolkit**, work from the cited evidence behind this row. [055, 2026] OSINT Techniques. Resources for Uncovering Online Information - 11th Edition (2024). [301, 2026] Official Intelligence Community strategy for open-source intelligence governance, integration, source discovery, data, tools, tradecraft, and workforce priorities. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **The Analyst's Toolkit**, build a **dissemination map with audience, caveat, marking, records, and feedback fields** for this cycle mapping and audience-aware product design topic. The artifact must name the source descriptor, the bounded claim about **Analyst's Toolkit**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **The Analyst's Toolkit** work as a **workload and decision-hygiene card** that states the evidence used, what stays uncertain, who reviews it, and when

to stop.

Misconception check. Correct the misconception that The Analyst's Toolkit: Hardware, Software, and Network Configuration establishes intent without reviewing alternative explanations.

Transfer task. Transfer **The Analyst's Toolkit** to a second module by preserving cycle mapping and audience-aware product design, changing the source evidence, and naming a new reviewer.

61.2.3 Information Architecture for Intelligence Work worked safe example: synthetic inputs, evidence, and review

Worked example: a synthetic analyst team rebuilds a storm-impact brief after discovering a stale requirement and overloaded reading queue. [251, 2026]; [268, 2026].

Triangulation anchors. In module 44's worked-example section, directly verified anchors for the **Governed Intelligence Cycle and Dissemination Architecture** lane include [Community, 2026]; [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026c]; [of the Director of National Intelligence, 2025a]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **analyst cognitive performance**. Learners use a **workload and decision-hygiene card** and keep this boundary visible: No productivity optimization may override safety, review, accessibility, rest, or records duties.

Frame. The classroom question centers on **Personal Knowledge Management (PKM) Systems for Intelligence Professionals**. Excluded actions stay explicit, and the **Dissemination-and-Marking Control Lens** planning question is: Which audience, release authority, marking vocabulary, records duty, and feedback loop governs this intelligence artifact?

Inputs. For the **Personal Knowledge Management Systems for Intelligence Professionals** scenario, use public weather bulletins, public infrastructure maps, historical outage summaries, and instructor-provided toy records. The Dissemination-and-Marking Control Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Personal Knowledge Management Systems for Intelligence Professionals**, students map the requirement, tag each source, separate observation from judgment, assign caveats, and record the dissemination audience. Pause whenever an inference about Personal Knowledge Management Systems for Intelligence Professionals appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Personal Knowledge Management Systems for Intelligence Professionals** classroom scenario; unit artifact = workload and decision-hygiene card; evidence = allowed inputs; method = cycle mapping and audience-aware product design; output = a one-page release-neutral brief with source descriptors, confidence language, caveats, and a feedback owner; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Personal Knowledge Management Systems for Intelligence Professionals** as "Dissemination-and-Marking Control Lens confirms it" is not enough. The revision ties the claim to cycle mapping and audience-aware product design, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Personal Knowledge Management Systems for Intelligence Professionals** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

61.2.4 Information Architecture for Intelligence Work practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Dissemination-and-Marking Control Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**.

Triangulation anchors. In module 44's practice-sequence section, directly verified anchors for the **Governed Intelligence Cycle and Dissemination Architecture** lane include [Community, 2026]; [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026c]; [of the Director of National Intelligence, 2025a]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Personal Knowledge Management Systems for Intelligence Professionals, Zettelkasten: German Note-Taking System for Researchers, Obsidian, Roam Research, LogSeq: PKM Tools for Analysts; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Governed Intelligence Cycle and Dissemination Architecture** lane.
2. Frame	Answer the lens question: Which audience, release authority, marking vocabulary, records duty, and feedback loop governs this intelligence artifact?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Personal Knowledge Management Systems for Intelligence Professionals: dissemination map with audience, caveat, marking, records, and feedback fields.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the workload and decision-hygiene card fields for Personal Knowledge Management Systems for Intelligence Professionals.	Unit profile note.	Evidence artifacts include workload signal, focus-block plan.
4. Challenge	Test the misconception that Personal Knowledge Management (PKM) Systems for Intelligence Professionals replaces human review whenever evidence looks plausible.	Failure-mode note.	The artifact applies the key distinction: separate intelligence work from ordinary research by naming authority, audience, caveats, and feedback.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

61.2.4.1 Information Architecture for Intelligence Work instructor notes: source reasoning, review points, and studio focus Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**. [251, 2026]; [268, 2026].

61.2.4.2 Information Architecture for Intelligence Work extension exercise: peer validation and refresh trigger review **Evidence anchor.** Section 61; [251, 2026].

Have learners swap artifacts and apply the **Dissemination-and-Marking Control Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**.

61.2.5 Information Architecture for Intelligence Work knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 61; [251, 2026].

1. Explain how **Personal Knowledge Management (PKM) Systems for Intelligence Professionals** is defined here; name the source descriptor that supports the definition.
2. Contrast **Personal Knowledge Management Systems for Intelligence Professionals** with **Zettelkasten: German Note-Taking System for Researchers** using the **Dissemination-and-Marking Control Lens** artifact fields.
3. Identify one failure mode from the **Governed Intelligence Cycle and Dissemination Architecture** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which requirement, source, or workflow step failed first when the team ran out of review time?
5. Correct this misconception: that Personal Knowledge Management (PKM) Systems for Intelligence Professionals replaces human review whenever evidence looks plausible.

61.2.5.1 Information Architecture for Intelligence Work answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Personal Knowledge Management Systems for Intelligence Professionals** without source evidence, uncertainty, or a safe transfer task.

61.3 Information Architecture for Intelligence Work assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 61; [251, 2026].

61.3.1 Information Architecture for Intelligence Work evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 61; [251, 2026].

61.3.2 Information Architecture for Intelligence Work transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 61; [251, 2026].

61.3.2.1 Information Architecture for Intelligence Work lineage and source tradition: profile, concepts, and first anchors This sits in the **Governed Intelligence Cycle and Dissemination Architecture** lineage: treating the intelligence cycle as a governed information system whose collection, processing, analysis, dissemination, evaluation, marking, and records obligations stay explicit. [251, 2026]; [268, 2026].

61.3.2.2 Information Architecture for Intelligence Work working model: inputs, constraints, transforms, outputs, and oversight Evidence anchor. Section 61; [251, 2026].
The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**, with provenance and reviewability throughout.

61.3.2.3 Information Architecture for Intelligence Work knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** requirements, audience needs, public-source evidence, caveats, and feedback signals. [251, 2026]; [268, 2026].
- **Transforms:** requirement framing, collection scoping, source evaluation, analytic judgment, dissemination, and feedback review.
- **Outputs:** release-neutral brief, audience map, caveat register, and feedback note.
- **Failure modes:** unscoped audiences, missing caveats, weak records, and product reuse without feedback.

61.3.2.4 Information Architecture for Intelligence Work transfer contracts: authority, evidence, tools, and auditable output Evidence anchor. Section 61; [251, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**.
- **Evidence contract:** keep the **Governed Intelligence Cycle and Dissemination Architecture** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as release-neutral brief, audience map, caveat register, and feedback note that another reviewer can audit.

61.3.2.5 Information Architecture for Intelligence Work profile emphasis and local focus: method stack and topic cluster Evidence anchor. Section 61; [251, 2026].
The matched profile emphasizes treating the intelligence cycle as a governed information system whose collection, processing, analysis, dissemination, evaluation, marking, and records obligations stay explicit. The method stack is cycle mapping, priority-to-product traceability, data-lifecycle mapping, classification vocabulary review, dissemination-caveat audit, customer feedback, and oversight checkpointing; the local topic cluster is **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**.

61.3.3 Information Architecture for Intelligence Work evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 61; [251, 2026].
Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Governed Intelligence Cycle and Dissemination Architecture** profile tells reviewers what evidence is strong enough for the module artifact built around **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**.

61.3.3.1 Information Architecture for Intelligence Work guide source spine: inherited keys and local citation roles Primary guide citations: [251, 2026]; [268, 2026]; [269, 2026]; [280, 2026]; [281, 2026]; [282, 2026]; [292, 2026]; [295, 2026]; [296, 2026]; [308, 2026]; [311, 2026]; [307, 2026]; [305, 2026]; [304, 2026]; [052, 2026]; [051, 2026]; [297, 2026]; [298, 2026]; [055, 2026]; [301, 2026]; [309, 2026]; [310, 2026]; [300, 2026].

61.3.3.2 Information Architecture for Intelligence Work verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [251, 2026]; [268, 2026].

Tier	What counts	How it is used
Source guide	[251, 2026]; [268, 2026]; [269, 2026]; [280, 2026]; [281, 2026]; [282, 2026]; [292, 2026]; [295, 2026]; [296, 2026]; [308, 2026]; [311, 2026]; [307, 2026]; [305, 2026]; [304, 2026]; [052, 2026]; [051, 2026]; [297, 2026]; [298, 2026]; [055, 2026]; [301, 2026]; [309, 2026]; [310, 2026]; [300, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 44's source-canon section, directly verified anchors for the **Governed Intelligence Cycle and Dissemination Architecture** lane include [Community, 2026]; [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026c]; [of the Director of National Intelligence, 2025a]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Maintenance rule: Perplexity may suggest candidates for **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers** and [251, 2026]; [268, 2026], but only directly verified source URLs are encoded as citations.

61.3.3.3 Information Architecture for Intelligence Work intelligence practice lens: evidence artifact and safety check Practice lens: **Dissemination-and-Marking Control Lens** for **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**. [251, 2026]; [268, 2026].

Planning question: Which audience, release authority, marking vocabulary, records duty, and feedback loop governs this intelligence artifact?

Evidence artifact: dissemination map with audience, caveat, marking, records, and feedback fields.

Validation rule: verify source authority, public/classification status, CAPCO-safe vocabulary, audience need, and records disposition before reuse. Applied to **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**.

Handoff contract: deliver release-neutral summaries, source metadata, marking rationale, and review ownership as separate fields.

Safety check: exclude classified content, live release decisions, source-method exposure, and improvised control markings.

61.3.3.4 Information Architecture for Intelligence Work runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 61; [251, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	44.99	44.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Information Architecture for Intelligence Work to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Bounded autonomy, procurement, incident-response, and assurance studio	44.101	44.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Information Architecture for Intelligence Work	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Model-card, recoverability, retention, and learner-support evidence package	44.102	44.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Information Architecture for Intelligence Work	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Personal Knowledge Management (PKM) Systems for Intelligence Professionals	44.1	44.1 Personal Knowledge Management (PKM) Systems for Intelligence Professionals	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Zettelkasten: German Note-Taking System for Researchers	44.1.1	44.1.1 Zettelkasten: German Note-Taking System for Researchers	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Obsidian, Roam Research, LogSeq: PKM Tools for Analysts	44.1.2	44.1.2 Obsidian, Roam Research, LogSeq: PKM Tools for Analysts	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Second Brain Methodology Applied to Intelligence Collection	44.1.3	44.1.3 Second Brain Methodology Applied to Intelligence Collection	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Information Diet and Source Hygiene	44.2	44.2 Information Diet and Source Hygiene	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Distraction Architecture: Designing Environments for Deep Analytical Work	44.3	44.3 Distraction Architecture: Designing Environments for Deep Analytical Work	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Collaborative Intelligence: Team Workflows, Shared Notes, Secure Platforms	44.4	44.4 Collaborative Intelligence: Team Workflows, Shared Notes, Secure Platforms	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
The Analyst's Toolkit: Hardware, Software, and Network Configuration	44.5	44.5 The Analyst's Toolkit: Hardware, Software, and Network Configuration	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings

61.3.3.5 Information Architecture for Intelligence Work reusable subsection contract: topic rows, artifacts, and safety duties Evidence anchor. Section 61; [251, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Personal Knowledge Management (PKM) Systems for Intelligence Professionals	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Zettelkasten: German Note-Taking System for Researchers	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Obsidian, Roam Research, LogSeq: PKM Tools for Analysts	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Second Brain Methodology Applied to Intelligence Collection	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Information Diet and Source Hygiene	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
Distraction Architecture: Designing Environments for Deep Analytical Work	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings

Lesson topic	Practice lens	Evidence artifact	Safety check
Collaborative Intelligence: Team Workflows, Shared Notes, Secure Platforms	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings
The Analyst's Toolkit: Hardware, Software, and Network Configuration	Dissemination-and-Marking Control Lens	dissemination map with audience, caveat, marking, records, and feedback fields	exclude classified content, live release decisions, source-method exposure, and improvised control markings

61.3.3.6 Information Architecture for Intelligence Work annotated source ledger: real titles and local contribution Each source cited by this **Governed Intelligence Cycle and Dissemination Architecture** module is paired below with its real title and a one-line note on what it contributes to **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**.

Source	Cited work	What it contributes	Status
[251, 2026]	European Data Governance Act	The European Commission page explaining the Data Governance Act, an EU regulation that became applicable in September 2023 to build trust in data sharing and ease reuse of data. It outlines four mechanisms: facilitating reuse of protected public-sector data, establishing trusted data intermediaries, enabling voluntary data sharing by citizens and businesses, and removing barriers to cross-sector and cross-border data use.	verified source-guide
[268, 2026]	Data Catalog Vocabulary (DCAT) Version 3	DCAT Version 3 is a W3C RDF vocabulary designed to facilitate interoperability between data catalogs published on the web, enabling organizations to describe datasets and data services using standardized terminology for improved discoverability and federated search. The specification organizes catalog metadata around seven core classes including Catalog, Dataset, Distribution, Data Service, and Dataset Series, drawing on established vocabularies such as Dublin Core and FOAF.	verified source-guide
[269, 2026]	Data on the Web Best Practices	A W3C Recommendation, "Data on the Web Best Practices," published January 31, 2017 by the Data on the Web Best Practices Working Group. It offers 35 best practices for publishing and consuming data on the Web, covering metadata, licensing and provenance, data quality, dataset versioning, persistent URIs, machine-readable formats, vocabulary reuse, access methods, preservation, and feedback.	verified source-guide
[280, 2026]	NIST SP 800-61 Rev. 3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management	NIST SP 800-61 Rev. 3, published April 2025, integrates incident response guidance into broader cybersecurity risk management aligned with the NIST Cybersecurity Framework 2.0, superseding the 2012 Rev. 2. The publication addresses cyber threat information sharing, incident handling and management practices, and procedures for detecting, responding to, and recovering from security incidents.	verified source-guide

Source	Cited work	What it contributes	Status
[281, 2026]	Artificial Intelligence Cybersecurity Challenges	An ENISA (European Union Agency for Cybersecurity) report published December 15, 2020 mapping the cybersecurity challenges of artificial intelligence. It defines AI scope through a lifecycle approach, identifies the assets requiring protection within AI ecosystems, and develops a threat taxonomy classified across lifecycle stages and asset categories.	verified source-guide
[282, 2026]	AI Research: Security and Resilience	A NIST page on AI research focused on security and resilience, framing these as core characteristics of trustworthy AI under the NIST AI Risk Management Framework.	verified source-guide
[292, 2026]	Assessing Risks and Impacts of AI (ARIA): Pilot Evaluation Report	The ARIA 0.1 pilot evaluation report documents NIST's methodology for systematically assessing AI applications for risks and societal impacts, using a multi-layered evaluation approach across five participating organizations and seven submitted AI applications. The pilot employed three evaluation scenarios and three testing levels: model testing, red teaming, and field testing, supplemented by dialogue annotation, tester questionnaires, and structured measurement trees.	verified source-guide
[295, 2026]	M-25-22: Driving Efficient Acquisition of Artificial Intelligence in Government	OMB Memorandum M-25-22 (April 3, 2025), Driving Efficient Acquisition of Artificial Intelligence in Government, issued under Executive Order 13960 and related directives. It provides guidance to federal agencies for acquiring effective and trustworthy AI in a timely, cost-effective manner, and rescinds and replaces earlier memorandum M-24-18.	verified source-guide
[296, 2026]	Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile	NIST AI 600-1, the Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, a cross-sectoral companion resource to the NIST AI RMF 1.0 issued pursuant to Executive Order 14110. It identifies risks that are unique to or amplified by generative AI and organizes suggested actions for managing those risks, mapped to the AI RMF functions.	verified source-guide
[308, 2026]	Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure	An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure.	verified source-guide
[311, 2026]	Countering Information Threats	An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering.	verified source-guide

Source	Cited work	What it contributes	Status
[307, 2026]	ICS Recommended Practices	Official CISA Industrial Control Systems recommended practices page for defensive ICS/OT safety, resilience, and incident-preparation guidance.	original source-guide
[305, 2026]	DevSecOps	Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support.	original source-guide
[304, 2026]	Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities	NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences.	verified source-guide
[052, 2026]	What is Open Source Intelligence & Top 10 Tools - Lampyre	This article defines open source intelligence as the practice of gathering information from publicly available data for security, business, and investigative purposes, drawing on websites, social media, government records, and public databases.	verified source-guide
[051, 2026]	Cited source (see bibliography)	See bibliography for scope.	original source-guide
[297, 2026]	Intelligence Community Directive 203: Analytic Standards	Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products.	original source-guide
[298, 2026]	Intelligence Community Directives	Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations.	original source-guide
[055, 2026]	IntelTechniques Books	OSINT Techniques. Resources for Uncovering Online Information - 11th Edition (2024).	original source-guide
[301, 2026]	The IC OSINT Strategy 2024-2026	Official Intelligence Community strategy for open-source intelligence governance, integration, source discovery, data, tools, tradecraft, and workforce priorities.	original source-guide
[309, 2026]	STIX Version 2.1	An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection.	verified source-guide
[310, 2026]	TAXII Version 2.1	The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe).	verified source-guide
[300, 2026]	MITRE ATLAS	MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy.	original source-guide

Where this sits. This module's overview is Section 61; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

61.3.4 Information Architecture for Intelligence Work governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 61; [251, 2026].

61.3.5 Information Architecture for Intelligence Work analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 44's governance-boundary section, directly verified anchors for the **Governed Intelligence Cycle and Dissemination Architecture** lane include [Community, 2026]; [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026c]; [of the Director of National Intelligence, 2025a]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **Governed Intelligence Cycle and Dissemination Architecture** for **Personal Knowledge Management (PKM) Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**. [251, 2026]; [268, 2026].

Curriculum topic spine: Personal Knowledge Management (PKM) Systems for Intelligence Professionals, **Zettelkasten: German Note-Taking System for Researchers**, **Obsidian, Roam Research, LogSeq: PKM Tools for Analysts**. **Verified anchor cluster:** [Community, 2026]; [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026c]; [of the Director of National Intelligence, 2025a]; [of the Director of National Intelligence, 2026b]; [General Services Administration et al., 2026]; [Privacy and Board, 2026].

Conceptual depth: treating the intelligence cycle as a governed information system whose collection, processing, analysis, dissemination, evaluation, marking, and records obligations stay explicit.

Method stack: cycle mapping, priority-to-product traceability, data-lifecycle mapping, classification vocabulary review, dissemination-caveat audit, customer feedback, and oversight checkpointing.

Composability contract: requirements, data provenance, analytic judgments, markings, dissemination permissions, records obligations, and feedback remain separable artifacts.

Known failure modes: cycle theater, undocumented dissemination, classification drift, unclear release authority, stale records assumptions, and feedback loops that hide bias.

Defensive boundary: cycle and marking material remains public-source and educational; it never handles classified content, live release decisions, or source-method exposure. Applied to **Personal Knowledge Management (PKM) Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**.

Anchor	Why it matters here
[Community, 2026]	Official public explanation of the intelligence cycle, collection disciplines, dissemination, evaluation, oversight, and partners. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2015]	Official ODNI analytic tradecraft standards directive. Checked as of 2026-05-21; role: source_quality_anchor.
[of the Director of National Intelligence, 2026c]	Official prioritization directive for translating national intelligence priorities into collection, analysis, risk management, and responsiveness evaluation. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2025a]	Official IC data-management directive for data governance, data stewardship, CDO authority, interoperability, and data lifecycle management. Checked as of 2026-05-21; role: curriculum_anchor.
[of the Director of National Intelligence, 2026b]	Official CAPCO register for classification and control-marking vocabulary, abbreviations, portion markings, and dissemination syntax. Checked as of 2026-05-21; role: curriculum_anchor.
[General Services Administration et al., 2026]	Official federal data-governance benchmark for data as a strategic asset, ethical governance, lifecycle practices, and learning culture. Checked as of 2026-05-21; role: curriculum_anchor.
[Privacy and Board, 2026]	Official oversight-report library for privacy, civil-liberties, surveillance, watchlisting, facial-recognition, and redress analysis. Checked as of 2026-05-21; role: curriculum_anchor.

61.3.5.1 Information Architecture for Intelligence Work evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **Governed Intelligence Cycle and Dissemination Architecture** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [251, 2026]; [268, 2026].

61.3.6 Information Architecture for Intelligence Work agentic boundary: assist, approve, block, and record

Evidence anchor. Section 61; [251, 2026].

AGEINT translation is bounded by the **Governed Intelligence Cycle and Dissemination Architecture** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**.

61.3.6.1 Information Architecture for Intelligence Work permitted defensive utility: curriculum uses and safe outputs **Evidence anchor.** Section 61; [251, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**.

61.3.6.2 Information Architecture for Intelligence Work excluded operational boundary: blocked actions and stop rules Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [251, 2026]; [268, 2026] and **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

61.3.7 Information Architecture for Intelligence Work governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 61; [251, 2026].

Governance is practiced as a gate on the **Governed Intelligence Cycle and Dissemination Architecture** lane. Learners use the **Dissemination-and-Marking Control Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**.

61.3.7.1 Information Architecture for Intelligence Work governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [251, 2026]; [268, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Governed Intelligence Cycle and Dissemination Architecture** failure modes and the **Dissemination-and-Marking Control Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

61.3.7.2 Information Architecture for Intelligence Work evidence package handoff: appendices, records, and reuse Evidence anchor. Section 61; [251, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Dissemination-and-Marking Control Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**.

61.3.7.3 Information Architecture for Intelligence Work current-source assurance: verified anchors and local artifact fit The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**. [251, 2026]; [268, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_intelligence_gov_how_ic_works` for **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**?	How the IC Works; lane `governed_intelligence_cycle`; checked 2026-05-21.	dissemination map with audience, caveat, marking, records, and feedback fields; Official public explanation of the intelligence cycle, collection disciplines, dissemination, evaluation, oversight, and partners.
What does the module inherit from `official_odni_icd_203` for **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**?	Intelligence Community Directive 203: Analytic Standards; lane `source_quality_spine`; checked 2026-05-21.	dissemination map with audience, caveat, marking, records, and feedback fields; Official ODNI analytic tradecraft standards directive.
What does the module inherit from `official_odni_icd_204` for **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**?	Intelligence Community Directive 204: National Intelligence Priorities Framework; lane `collection_management`; checked 2026-05-21.	dissemination map with audience, caveat, marking, records, and feedback fields; Official prioritization directive for translating national intelligence priorities into collection, analysis, risk management, and responsiveness evaluation.
What does the module inherit from `official_odni_icd_504` for **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**?	Intelligence Community Directive 504: Intelligence Community Data Management; lane `ai_ethics_data_governance`; checked 2026-05-21.	dissemination map with audience, caveat, marking, records, and feedback fields; Official IC data-management directive for data governance, data stewardship, CDO authority, interoperability, and data lifecycle management.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 61; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

61.3.8 Information Architecture for Intelligence Work assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 61; [251, 2026].

61.3.9 Information Architecture for Intelligence Work assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 61; [251, 2026].

61.3.9.1 Information Architecture for Intelligence Work capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**.
Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers** and [251, 2026]; [268, 2026].

61.3.9.2 Information Architecture for Intelligence Work instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers** and [251, 2026]; [268, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

61.3.9.3 Information Architecture for Intelligence Work assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Personal Knowledge Management (PKM) Systems for Intelligence Professionals	Completed **dissemination map with audience, caveat, marking, records, and feedback fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Zettelkasten: German Note-Taking System for Researchers	Completed **dissemination map with audience, caveat, marking, records, and feedback fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Obsidian, Roam Research, LogSeq: PKM Tools for Analysts	Completed **dissemination map with audience, caveat, marking, records, and feedback fields** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

61.3.10 Information Architecture for Intelligence Work refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [251, 2026]; [268, 2026] and **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**.

61.3.10.1 Information Architecture for Intelligence Work refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**. The local signals begin with [251, 2026]; [268, 2026].

61.3.10.2 Information Architecture for Intelligence Work claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**, and the source spine for these checks begins with [251, 2026]; [268, 2026].

61.3.11 Information Architecture for Intelligence Work reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [251, 2026]; [268, 2026].
Triangulation anchors. In module 44's review-checklist section, directly verified anchors for the **Governed Intelligence Cycle and Dissemination Architecture** lane include [Community, 2026]; [of the Director of National Intelligence, 2015]; [of the Director of National Intelligence, 2026c]; [of the Director of National Intelligence, 2025a]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers**. [251, 2026]; [268, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

61.3.12 Information Architecture for Intelligence Work learning-path links: module map, overview, and curriculum atlas

Follow the cross-links to move between **Personal Knowledge Management Systems for Intelligence Professionals; Zettelkasten: German Note-Taking System for Researchers** and the rest of the curriculum without losing the source spine: orientation first, then the parent unit, then the modules on either side. Primary sources: [251, 2026]; [268, 2026].

Section 2, Section 59, Section 60, Section 62

62 INDUSTRIAL AND CYBER-PHYSICAL INTELLIGENCE

62.1 INDUSTRIAL AND CYBER-PHYSICAL INTELLIGENCE learning spine and source route: unit purpose, module order, and evidence handoff

Evidence anchor. Section 62; [255, 2026].

62.1.1 safety-aware ICS and OT intelligence discipline spine: domain question and learning focus

Evidence anchor. Section 62; [255, 2026].
This unit teaches **safety-aware ICS and OT intelligence**. ICS/OT lessons connect cyber observations to engineering state, consequence, operator decision, recovery evidence, and safety governance.

62.1.2 safety-aware ICS and OT intelligence source-use contract: citation roles and evidence limits

Evidence anchor. Section 62; [255, 2026].
Use CISA ICS, NIST secure-development, DevSecOps, and MITRE anchors for defensive coverage and controlled release claims.

62.1.3 safety-aware ICS and OT intelligence practice artifact: recurring packet and retained evidence

Evidence anchor. Section 62; [255, 2026].
The recurring practice artifact is a **cyber-physical tabletop evidence packet** that draws on asset-consequence map, operator decision log, recovery evidence, and safety stop card. The unit keeps its learning spine explicit. Learners map assets to consequence, classify observations defensively, and preserve recovery evidence.

62.1.4 safety-aware ICS and OT intelligence safety boundary: accountable, synthetic, and evidence-bounded limits

No live device control, unsafe process change, exploit sequence, evasion, or operational response.
This unit introduces the part's governing question, evidence artifacts, source-support spine, and capstone thread before the individual modules begin. [255, 2026]; [256, 2026].
Learners carry one unit capstone thread through the part: define an accountable intelligence question, bind it to source-quality constraints, produce a reviewable artifact, test the artifact against failure modes, and hand it off with enough context for another analyst or instructor to audit. The capstone remains public, synthetic, or owned-lab throughout; its first source anchors are [255, 2026]; [256, 2026].
This unit's deliverables are a source-canon card, claim/evidence ledger, safe-practice lab packet, failure-mode note, instructor rubric, and debrief memo. The full source-lane and evidence-package ledgers appear in the orientation and appendices; this unit introduction keeps only the learner-facing spine for [255, 2026]; [256, 2026].
This unit's safety gates are scope authorization, rights review, data provenance, tool allowlisting, human oversight, rollback, and evidence-bounded output. A missing gate turns the activity into a tabletop, audit, or written governance exercise until the gate is restored against [255, 2026]; [256, 2026].
Capstone thread:

Phase	Artifact	Review gate
Question	accountable learning question and excluded-action list	instructor confirms scope, allowed data, and rights impact
Source canon	source-lane map with guide citations, verified anchors, and refresh dates	citation keys resolve and source identity lock remains stable
Evidence ledger	claim, evidence, uncertainty, confidence, and reviewer register	every material claim has a source, caveat, and owner
Safe lab	synthetic or public dataset packet, tool allowlist, and stop conditions	no live target, private data, external action, or unsafe cyber-physical step
Assurance	evaluation rubric, failure-mode drill, rights map, and remediation note	human reviewer signs off before presentation or reuse
Debrief	capstone memo with lessons, residual risk, refresh triggers, and handoff owner	all unresolved questions and future approvals are explicit

Research lane: ICS/OT Cyber-Physical Defense and Tabletop Readiness. Core anchors: [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]. Conceptual focus: defensive intelligence for safety-critical environments where availability, engineering state, and physical consequence matter. Composability contract: separate cyber indicators, engineering observations, safety impacts, operator decisions, and recovery actions. **Practice lens:** Cyber-Physical Readiness Lens; Which asset, architecture record, consequence, operator decision, and recovery path is being exercised defensively? [255, 2026]; [256, 2026].

62.1.5 INDUSTRIAL AND CYBER-PHYSICAL INTELLIGENCE visual navigation and module map: evidence flow, order, and safety cues

The unit uses Figure 134 and Figure 135 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 61, Section 63.

62.1.6 INDUSTRIAL AND CYBER-PHYSICAL INTELLIGENCE module roster and source-lane inventory: citations, lanes, and learner route

Module	Section reference	Source spine
Industrial Control Systems (ICS) and Operational Technology	Section 63	[255, 2026]; [256, 2026]; [270, 2026]; [273, 2026]; [276, 2026]; [285, 2026]; [286, 2026]; [290, 2026]; [294, 2026]; [208, 2026]; [209, 2026]; [210, 2026]; [211, 2026]; [212, 2026].
MITRE ATT&CK for ICS	Section 64	[255, 2026]; [257, 2026]; [261, 2026]; [274, 2026]; [278, 2026]; [280, 2026]; [287, 2026]; [288, 2026]; [295, 2026]; [213, 2026]; [214, 2026]; [215, 2026]; [216, 2026].

Module	Section reference	Source spine
Historical ICS Cyber Incidents: Intelligence Analysis	Section 65	[252, 2026]; [255, 2026]; [270, 2026]; [279, 2026]; [282, 2026]; [284, 2026]; [289, 2026]; [291, 2026]; [296, 2026]; [217, 2026]; [218, 2026]; [219, 2026]; [220, 2026].
Threat Intelligence Sharing for Critical Infrastructure	Section 66	[253, 2026]; [258, 2026]; [261, 2026]; [275, 2026]; [276, 2026]; [283, 2026]; [286, 2026]; [293, 2026]; [295, 2026]; [077, 2026]; [218, 2026]; [307, 2026]; [305, 2026]; [304, 2026].
AGEINT Applied to ICS and Cyber-Physical Intelligence	Section 67	[255, 2026]; [256, 2026]; [257, 2026]; [273, 2026]; [274, 2026]; [275, 2026]; [286, 2026]; [287, 2026]; [292, 2026]; [213, 2026]; [307, 2026]; [305, 2026]; [304, 2026]; [299, 2026]; [306, 2026]; [312, 2026]; [300, 2026].

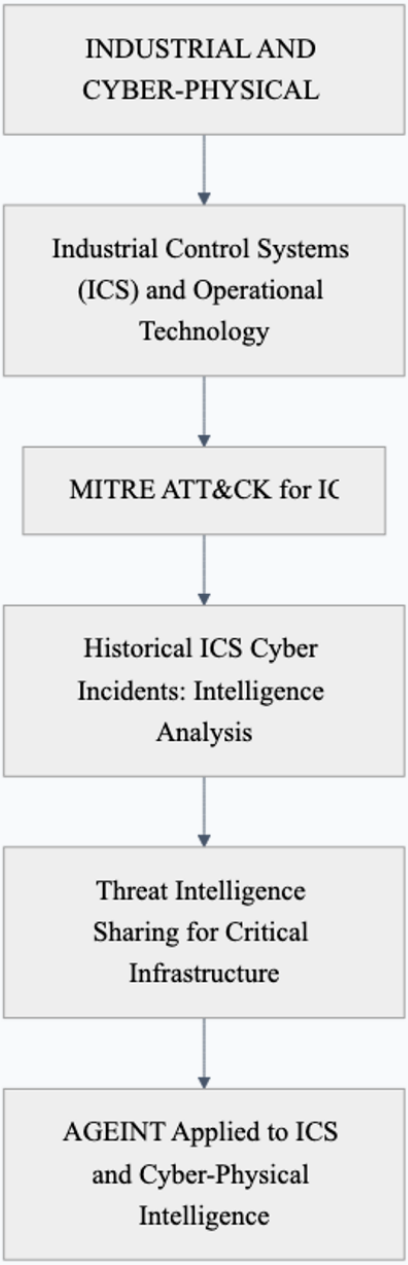


Figure 134: The unit module map traces the part's chapters as a linear reading sequence. In the industrial and cyber physical intelligence section, it lets readers compare 5 module nodes in the unit's ordered, source-backed reading sequence from its first module to its last so the visual functions as a traceable course aid rather than an unscoped assertion.

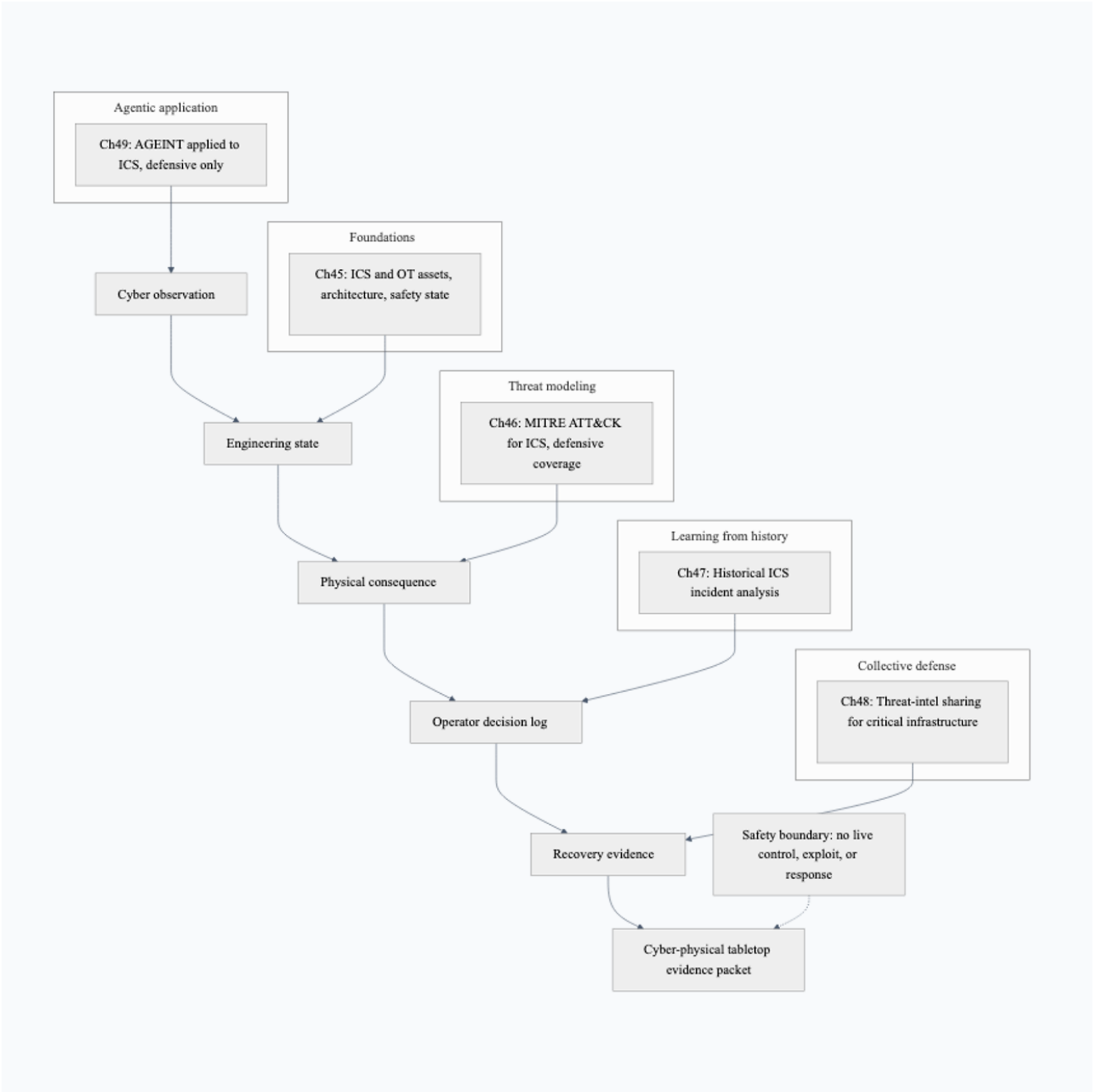


Figure 135: This part builds a defensive chain from cyber observation through engineering state, physical consequence, operator decision, and recovery evidence, with each of the five chapters feeding a stage and a hard safety boundary forbidding live control, exploitation, or operational response.

63 Industrial Control Systems (ICS) and Operational Technology

63.0.1 Industrial Control Systems (ICS) and Operational Technology figures and course links: visual evidence, source flow, and navigation

The module uses Figure 136, Figure 137, and Figure 134 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.

Navigation links: Section 2, Section 62, Section 64.

This module teaches the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane through a bounded, source-backed coursebook chapter. [255, 2026]; [256, 2026].

63.1 ICS/OT Cyber-Physical Defense and Tabletop Readiness frame for Industrial Control Systems (ICS) and Operational Technology: source context, topic focus, and reader task

Evidence anchor. Section 63; [255, 2026].

63.1.1 Industrial Control Systems (ICS) and Operational Technology orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 63; [255, 2026].

63.1.2 Industrial Control Systems (ICS) and Operational Technology conceptual primer: source context, core model, and reader task

This chapter teaches ICS/OT intelligence as safety-aware defensive reasoning: asset state, engineering consequence, operator decision, and recovery evidence matter as much as cyber indicators. The chapter uses **Cyber-Physical Readiness Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition**.

The central distinction is to separate cyber analysis from unsafe process control or live operational action. Core topics include **ICS Architecture: SCADA, DCS, PLC, HMI — Definitions and Roles; SCADA: Supervisory Control and Data Acquisition — Large Geographic Systems; DCS: Distributed Control Systems — Chemical, Refining, Power**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.

Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [255, 2026]; [256, 2026].

Learners move from vocabulary and the **Cyber-Physical Readiness Lens** distinction through topic lessons on **ICS Architecture: SCADA, DCS, PLC, HMI — Definitions and Roles** with evidence and misconception checks, then assemble a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** with safety and rights gates.

63.1.3 Industrial Control Systems (ICS) and Operational Technology learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 63; [255, 2026].

- Connect **ICS Architecture: SCADA, DCS, PLC, HMI — Definitions and Roles and SCADA: Supervisory Control and Data Acquisition — Large Geographic Systems** to **ICS/OT Cyber-Physical Defense and Tabletop Readiness** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate cyber analysis from unsafe process control or live operational action; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as IT-first assumptions, unsafe automation, untested shutdown logic, poor remote-access control, and missing after-action learning, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: all ICS work remains tabletop, lab, or accountable defensive review; no exploitation, unsafe process manipulation, or live control actions.

63.1.4 Industrial Control Systems (ICS) and Operational Technology core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 63; [255, 2026].

Term	Working definition
Engineering state	the physical or process condition that gives cyber evidence safety meaning
Consequence	the operational, safety, environmental, or service effect of a condition
Defense in depth	layered prevention, detection, response, and recovery controls
Tabletop inject	a synthetic event used to rehearse decisions without touching live systems
Recovery evidence	proof that a safe state, service, or learning objective was restored
ICS Architecture: SCADA, DCS, PLC, HMI —…	Key terms: ICS, Architecture, SCADA.
SCADA: Supervisory Control and Data Acquisition…	Key terms: SCADA, Supervisory, Control.

Figure 136: This diagram teaches the Purdue-aligned segmentation of an industrial control environment, showing how a brokered DMZ separates IT from OT and how an independent safety system forms the last protective layer. It is anchored to the industrial and cyber physical intelligence / industrial control systems ics and operational technology section; use it to inspect ICS Defensive Zone Model Purdue-aligned segmentation and the safety boundary, Enterprise zone, Level 5-4 business and enterprise IT, and Industrial DMZ while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

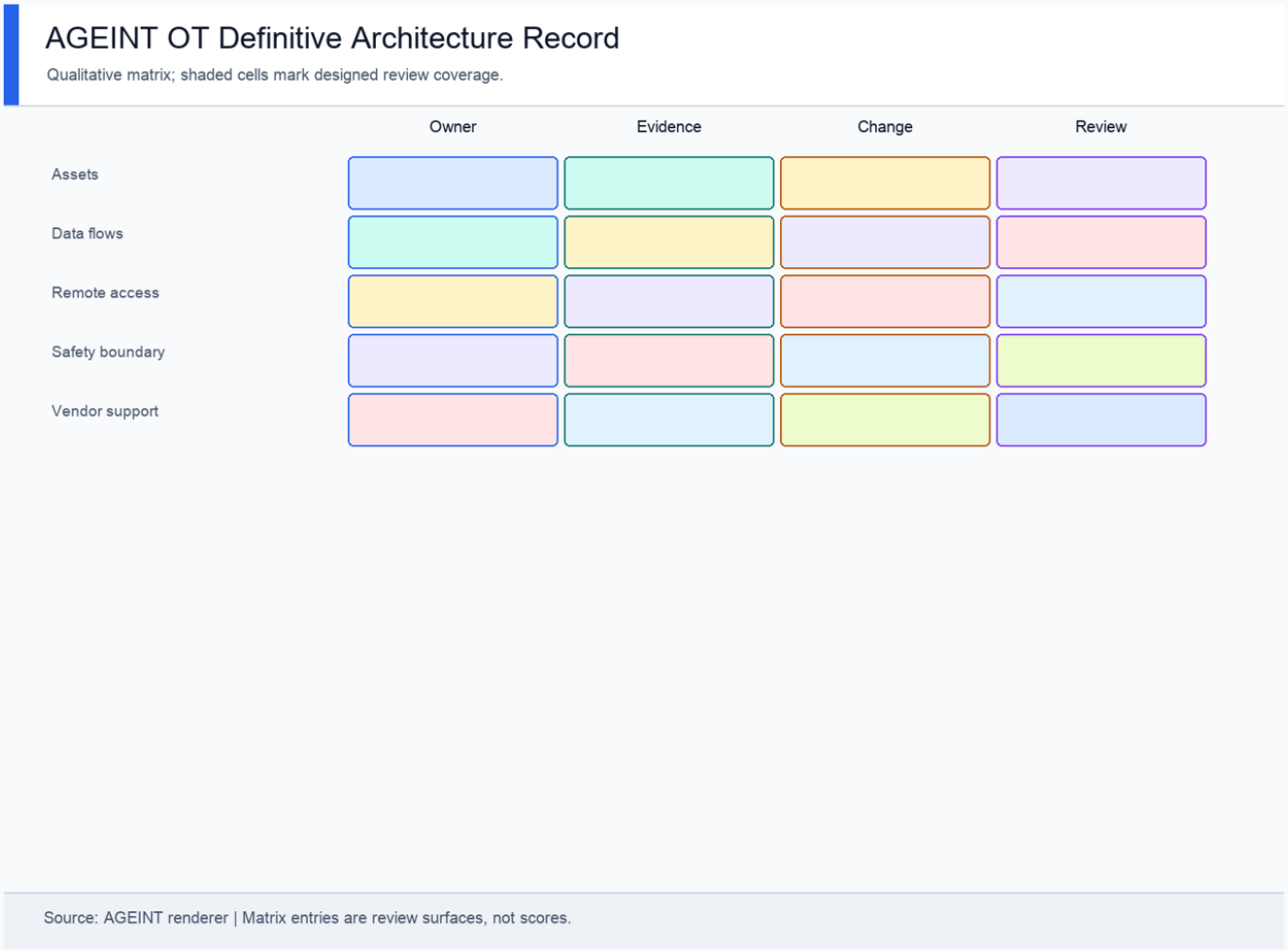


Figure 137: The OT architecture record ties assets, communications, owners, change evidence, and review cadence together. It is anchored to the industrial and cyber physical intelligence / industrial control systems ics and operational technology section; use it to inspect ot definitive architecture record labels, source records, review gates, refresh cues, and reader-use boundaries while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

63.2 Cyber-Physical Readiness Lens path for Industrial Control Systems (ICS) and Operational Technology: lesson cluster, safe artifact, and review

Evidence anchor. Section 63; [255, 2026].

63.2.1 Industrial Control Systems (ICS) and Operational Technology practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 63; [255, 2026].

63.2.2 Industrial Control Systems (ICS) and Operational Technology topic lessons: source-backed concepts and transfer tasks

This module builds ICS/OT intelligence as safety-aware defensive reasoning: asset state, engineering consequence, operator decision, and recovery evidence matter as much as cyber indicators. The sequence opens with **ICS Architecture: SCADA, DCS, PLC, HMI — Definitions and Roles**, **SCADA: Supervisory Control and Data Acquisition — Large Geographic Systems**, **DCS: Distributed Control Systems — Chemical, Refining, Power** and applies the **Cyber-Physical Readiness Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 134; module overview Section 63; curriculum atlas Section 2.

Triangulation anchors. In module 45's topic-lessons section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

63.2.2.1 Lesson 1: ICS Architecture: SCADA, DCS, PLC, HMI — Definitions and Roles

Concept. ICS Architecture: SCADA, DCS, PLC, HMI — Definitions and Roles maps industrial assets, safety interlocks, operator roles, and consequence before any cyber-physical inference.

Why it matters. ICS Architecture: SCADA, DCS, PLC, HMI — Definitions and Roles connects classroom vocabulary to ICS/OT Cyber-Physical Defense and Tabletop Readiness practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. ICS Architecture: SCADA, DCS, PLC, HMI — Definitions and Roles rests on [208, 2026] and [209, 2026]. Its anchor reference records: This article provides a comprehensive overview of cybersecurity for Industrial Control Systems, covering SCADA, distributed control systems, and programmable logic controllers as they have evolved from isolated architectures to networked, cloud-connected deployments. Use them for the working definition that **ICS Architecture: SCADA, DCS, PLC, HMI — Definitions and Roles** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. For **ICS Architecture: SCADA, DCS, PLC, HMI — Definitions and Roles**, work from the cited evidence behind this row. [208, 2026] This article provides a comprehensive overview of cybersecurity for Industrial Control Systems, covering SCADA, distributed control systems, and programmable logic controllers as they have evolved from isolated architectures to networked, cloud-connected deployments. [209, 2026] A glossary entry from the cybersecurity company Bitsight explaining Industrial Control Systems (ICS), defined as integrated hardware and software used to control, monitor, and automate industrial processes across manufacturing, energy, and critical infrastructure. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **ICS Architecture**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must name the source descriptor, the bounded claim about **ICS Architecture**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **ICS Architecture: SCADA, DCS, PLC, HMI — Definitions and Roles** work as a **cyber-physical tabletop evidence packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that ICS Architecture: SCADA, DCS, PLC, HMI — Definitions and Roles establishes intent without reviewing alternative explanations.

Transfer task. Transfer **ICS Architecture: SCADA, DCS, PLC, HMI — Definitions and Roles** to a second module by preserving safety-aware tabletop readiness and defensive coverage review, changing the source evidence, and naming a new reviewer.

63.2.2.2 Lesson 2: SCADA: Supervisory Control and Data Acquisition — Large Geographic Systems

Concept. SCADA: Supervisory Control and Data Acquisition — Large Geographic Systems maps industrial assets, safety interlocks, operator roles, and consequence before any cyber-physical inference.

Why it matters. SCADA: Supervisory Control and Data Acquisition — Large Geographic Systems matters in the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane because safety-aware tabletop readiness and defensive coverage evidence must stay separate from judgment; IT-first assumptions is a common failure.

Source support. SCADA: Supervisory Control and Data Acquisition — Large Geographic Systems rests on [209, 2026]. The most specific cited work observes: A glossary entry from the cybersecurity company Bitsight explaining Industrial Control Systems (ICS), defined as integrated hardware and software used to control, monitor, and automate industrial processes across manufacturing, energy, and critical infrastructure. Use it for fixing what **SCADA: Supervisory Control and Data Acquisition — Large Geographic Systems** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. Read **SCADA: Supervisory Control and Data Acquisition — Large Geographic Systems** against the works cited for this row. [209, 2026] A glossary entry from the cybersecurity company Bitsight explaining Industrial Control Systems (ICS), defined as integrated hardware and software used to control, monitor, and automate industrial processes across manufacturing, energy, and critical infrastructure. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **SCADA**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must name the source descriptor, the bounded claim about **SCADA**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **SCADA: Supervisory Control and Data Acquisition — Large Geographic Systems** work as a **cyber-physical tabletop evidence packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that SCADA: Supervisory Control and Data Acquisition — Large Geographic Systems replaces human review whenever evidence looks plausible.

Transfer task. Transfer **SCADA: Supervisory Control and Data Acquisition — Large Geographic Systems** to a second module by preserving safety-aware tabletop readiness and defensive coverage review, changing the source evidence, and naming a new reviewer.

63.2.2.3 Lesson 3: DCS: Distributed Control Systems — Chemical, Refining, Power

Concept. DCS: Distributed Control Systems — Chemical, Refining, Power maps industrial assets, safety interlocks, operator roles, and consequence before any cyber-physical inference.

Why it matters. Analysts use **DCS: Distributed Control Systems — Chemical, Refining, Power** to separate cyber analysis from unsafe process control or live operational action. A defensible treatment names the judgment it enables for safety-aware tabletop readiness and defensive coverage review, the proof limit that IT-first assumptions would otherwise hide, and the reviewer accountable for challenge.

Source support. DCS: Distributed Control Systems — Chemical, Refining, Power rests on [209, 2026]. The closest source to this row notes: A glossary entry from the cybersecurity company Bitsight explaining Industrial Control Systems (ICS), defined as integrated hardware and software used to control, monitor, and automate industrial processes across manufacturing, energy, and critical infrastructure. Use it for fixing what **DCS: Distributed Control Systems — Chemical, Refining, Power** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. For **DCS: Distributed Control Systems — Chemical, Refining, Power**, reason from the sources cited in this row. [209, 2026] A glossary entry from the cybersecurity company Bitsight explaining Industrial Control Systems (ICS), defined as integrated hardware and software used to control, monitor, and automate industrial processes across manufacturing, energy, and critical infrastructure. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **DCS**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must name the source descriptor, the bounded claim about **DCS**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **DCS: Distributed Control Systems — Chemical, Refining, Power** work as a **cyber-physical tabletop evidence packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that DCS: Distributed Control Systems — Chemical, Refining, Power can be used while ignoring the rule to separate cyber analysis from unsafe process control or live operational action.

Transfer task. Transfer **DCS: Distributed Control Systems — Chemical, Refining, Power** to a second module by preserving safety-aware tabletop readiness and defensive coverage review, changing the source evidence, and naming a new reviewer.

63.2.2.4 Lesson 4: PLC: Programmable Logic Controllers — Field-Level Execution

Concept. PLC: Programmable Logic Controllers — Field-Level Execution maps industrial assets, safety interlocks, operator roles, and consequence before any cyber-physical inference.

Why it matters. Without explicit treatment of **PLC: Programmable Logic Controllers — Field-Level Execution**, IT-first assumptions undermines safety-aware tabletop readiness and defensive coverage review; the lesson builds the habit to separate cyber analysis from unsafe process control or live operational action.

Source support. PLC: Programmable Logic Controllers — Field-Level Execution rests on [209, 2026]. The closest source to this row notes: A glossary entry from the cybersecurity company Bitsight explaining Industrial Control Systems (ICS), defined as integrated hardware and software used to control, monitor, and automate industrial processes across manufacturing, energy, and critical infrastructure. Use it for fixing what **PLC: Programmable Logic Controllers — Field-Level Execution** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. For **PLC: Programmable Logic Controllers — Field-Level Execution**, reason from the sources cited in this row. [209, 2026] A glossary entry from the cybersecurity company Bitsight explaining Industrial Control Systems (ICS), defined as integrated hardware and software used to control, monitor, and automate industrial processes across manufacturing, energy, and critical infrastructure. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **PLC**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must name the source descriptor, the bounded claim about **PLC**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **PLC: Programmable Logic Controllers — Field-Level Execution** work as a **cyber-physical tabletop evidence packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that PLC: Programmable Logic Controllers — Field-Level Execution is optional whenever separate cyber analysis from unsafe process control or live operational action feels inconvenient.

Transfer task. Transfer **PLC: Programmable Logic Controllers — Field-Level Execution** to a second module by preserving safety-aware tabletop readiness and defensive coverage review, changing the source evidence, and naming a new reviewer.

63.2.2.5 Lesson 5: OT vs. IT: Fundamental Security Philosophy Differences

Concept. OT vs. IT: Fundamental Security Philosophy Differences applies OT, IT, Fundamental within ICS/OT Cyber-Physical Defense and Tabletop Readiness: learners use separate cyber analysis from unsafe process control or live operational action and safety-aware tabletop readiness and defensive coverage review evidence before any judgment moves forward.

Why it matters. OT vs. IT: Fundamental Security Philosophy Differences connects classroom vocabulary to ICS/OT Cyber-Physical Defense and Tabletop Readiness practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. OT vs. IT: Fundamental Security Philosophy Differences rests on [209, 2026] and [210, 2026]. The closest source to this row notes: A glossary entry from the cybersecurity company Bitsight explaining Industrial Control Systems (ICS), defined as integrated hardware and software used to control, monitor, and automate industrial processes across manufacturing, energy, and critical infrastructure. Use them for the claim that **OT vs. IT: Fundamental Security Philosophy Differences** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. For **OT vs. IT: Fundamental Security Philosophy Differences**, reason from the sources cited in this row. [209, 2026] A glossary entry from the cybersecurity company Bitsight explaining Industrial Control Systems (ICS), defined as integrated hardware and software used to control, monitor, and automate industrial processes across manufacturing, energy, and critical infrastructure. [210, 2026] A Palo Alto Networks Cyberpedia article explaining the relationship among operational technology (OT), industrial control system (ICS), and SCADA security. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **OT vs. IT**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must name the source descriptor, the bounded claim about **OT vs IT**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **OT vs. IT: Fundamental Security Philosophy Differences** work as a **cyber-physical tabletop evidence packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that OT vs. IT: Fundamental Security Philosophy Differences establishes intent without reviewing alternative explanations.

Transfer task. Transfer **OT vs. IT: Fundamental Security Philosophy Differences** to a second module by preserving safety-aware tabletop readiness and defensive coverage review, changing the source evidence, and naming a new reviewer.

63.2.2.6 Lesson 6: Air-Gap Erosion: The Digital Transformation Vulnerability

Concept. Air-Gap Erosion: The Digital Transformation Vulnerability treats the vulnerability record as an assurance case: severity, affected component, provenance, mitigation status, and uncertainty stay separate.

Why it matters. Air-Gap Erosion: The Digital Transformation Vulnerability matters in the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane because safety-aware tabletop readiness and defensive coverage evidence must stay separate from judgment; IT-first assumptions is a common failure.

Source support. Air-Gap Erosion: The Digital Transformation Vulnerability rests on [209, 2026]. The closest source to this row notes: A glossary entry from the cybersecurity company Bitsight explaining Industrial Control Systems (ICS), defined as integrated hardware and software used to control, monitor, and automate industrial processes across manufacturing, energy, and critical infrastructure. Use it for fixing what **Air-Gap Erosion: The Digital Transformation Vulnerability** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. Ground **Air-Gap Erosion: The Digital Transformation Vulnerability** in the evidence the row cites. [209, 2026] A glossary entry from the cybersecurity company Bitsight explaining Industrial Control Systems (ICS), defined as integrated hardware and software used to control, monitor, and automate industrial processes across manufacturing, energy, and critical infrastructure. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Air-Gap Erosion**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must name the source descriptor, the bounded claim about **Air-Gap Erosion**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Air-Gap Erosion: The Digital Transformation Vulnerability** work as a **cyber-physical tabletop evidence packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that Air-Gap Erosion: The Digital Transformation Vulnerability replaces human review whenever evidence looks plausible.

Transfer task. Transfer **Air-Gap Erosion: The Digital Transformation Vulnerability** to a second module by preserving safety-aware tabletop readiness and defensive coverage review, changing the source evidence, and naming a new reviewer.

63.2.2.7 Lesson 7: Securing ICS: Components, Protocols, Performance, Vulnerability Concept. Securing ICS: Components, Protocols, Performance, Vulnerability treats the vulnerability record as an assurance case: severity, affected component, provenance, mitigation status, and uncertainty stay separate.

Why it matters. Analysts use **Securing ICS: Components, Protocols, Performance, Vulnerability** to separate cyber analysis from unsafe process control or live operational action. A defensible treatment names the judgment it enables for safety-aware tabletop readiness and defensive coverage review, the proof limit that IT-first assumptions would otherwise hide, and the reviewer accountable for challenge.

Source support. Securing ICS: Components, Protocols, Performance, Vulnerability rests on [208, 2026]. The lead source's own note reads: This article provides a comprehensive overview of cybersecurity for Industrial Control Systems, covering SCADA, distributed control systems, and programmable logic controllers as they have evolved from isolated architectures to networked, cloud-connected deployments. Use it for fixing what **Securing ICS: Components, Protocols, Performance, Vulnerability** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. For **Securing ICS: Components, Protocols, Performance, Vulnerability**, work from the cited evidence behind this row. [208, 2026] This article provides a comprehensive overview of cybersecurity for Industrial Control Systems, covering SCADA, distributed control systems, and programmable logic controllers as they have evolved from isolated architectures to networked, cloud-connected deployments. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Securing ICS**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must name the source descriptor, the bounded claim about **Securing ICS**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Securing ICS: Components, Protocols, Performance, Vulnerability** work as a **cyber-physical tabletop evidence packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that Securing ICS: Components, Protocols, Performance, Vulnerability can be used while ignoring the rule to separate cyber analysis from unsafe process control or live operational action.

Transfer task. Transfer **Securing ICS: Components, Protocols, Performance, Vulnerability** to a second module by preserving safety-aware tabletop readiness and defensive coverage review, changing the source evidence, and naming a new reviewer.

63.2.2.8 Lesson 8: 2026 Cybersecurity Guide to ICS (Claroty) Concept. 2026 Cybersecurity Guide to ICS (Claroty) applies Cybersecurity, Guide, ICS within ICS/OT Cyber-Physical Defense and Tabletop Readiness: learners use separate cyber analysis from unsafe process control or live operational action and safety-aware tabletop readiness and defensive coverage review evidence before any judgment moves forward.

Why it matters. Without explicit treatment of **2026 Cybersecurity Guide**, IT-first assumptions undermines safety-aware tabletop readiness and defensive coverage review; the lesson builds the habit to separate cyber analysis from unsafe process control or live operational action.

Source support. 2026 Cybersecurity Guide to ICS (Claroty) rests on [211, 2026]. Its anchor reference records: It identifies challenges including an expanded attack surface, legacy systems lacking modern protections, third-party access gaps, patching delays due to uptime requirements, and advanced adversaries targeting ICS. Use it for fixing what **2026 Cybersecurity Guide to ICS (Claroty)** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. For **2026 Cybersecurity Guide**, work from the cited evidence behind this row. [211, 2026] A Claroty guide to securing industrial control systems (ICS) amid IT and operational technology convergence. It identifies challenges including an expanded attack surface, legacy systems lacking modern protections, third-party access gaps, patching delays due to uptime requirements, and advanced adversaries targeting ICS. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **2026 Cybersecurity Guide**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must name the source descriptor, the bounded claim about **Cybersecurity Guide to ICS**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **2026 Cybersecurity Guide** work as a **cyber-physical tabletop evidence packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that 2026 Cybersecurity Guide to ICS (Claroty) is optional whenever separate cyber analysis from unsafe process control or live operational action feels inconvenient.

Transfer task. Transfer **2026 Cybersecurity Guide** to a second module by preserving safety-aware tabletop readiness and defensive coverage review, changing the source evidence, and naming a new reviewer.

63.2.2.9 Lesson 9: OT vs. ICS vs. SCADA Security (Palo Alto Networks) Concept. OT vs. ICS vs. SCADA Security (Palo Alto Networks) maps industrial assets, safety interlocks, operator roles, and consequence before any cyber-physical inference.

Why it matters. Analysts use **OT vs. ICS vs. SCADA Security (Palo Alto Networks)** to separate cyber analysis from unsafe process control or live operational action. A defensible treatment names the judgment it enables for safety-aware tabletop readiness and defensive coverage review, the proof limit that IT-first assumptions would otherwise hide, and the reviewer accountable for challenge.

Source support. OT vs. ICS vs. SCADA Security (Palo Alto Networks) rests on [210, 2026]. The most specific cited work observes: A Palo Alto Networks Cyberpedia article explaining the relationship among operational technology (OT), industrial control system (ICS), and SCADA security. Use it for pinning down the scope of **OT vs. ICS vs. SCADA Security (Palo Alto Networks)**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. Ground **OT vs. ICS vs. SCADA Security (Palo Alto Networks)** in the evidence the row cites. [210, 2026] A Palo Alto Networks Cyberpedia article explaining the relationship among operational technology (OT), industrial control system (ICS), and SCADA security. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **OT vs. ICS vs. SCADA Security (Palo Alto Networks)**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must name the source descriptor, the bounded claim about **OT vs ICS vs SCADA**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape this subject work as a **cyber-physical tabletop evidence packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that OT vs. ICS vs. SCADA Security (Palo Alto Networks) establishes intent without reviewing alternative explanations.

Transfer task. Transfer **OT vs. ICS vs. SCADA Security (Palo Alto Networks)** to a second module by preserving safety-aware tabletop readiness and defensive coverage review, changing the source evidence, and naming a new reviewer.

63.2.2.10 Lesson 10: Operational Technology Cybersecurity (Idaho National Laboratory) Concept. Operational Technology Cybersecurity (Idaho National Laboratory) maps industrial assets, safety interlocks, operator roles, and consequence before any cyber-physical inference.

Why it matters. Analysts use **Operational Technology Cybersecurity (Idaho National Laboratory)** to separate cyber analysis from unsafe process control or live operational action. A defensible treatment names the judgment it enables for safety-aware tabletop readiness and defensive coverage review, the proof limit that IT-first assumptions would otherwise hide, and the reviewer accountable for challenge.

Source support. Operational Technology Cybersecurity (Idaho National Laboratory) rests on [212, 2026]. Use it for the working definition that **Operational Technology Cybersecurity (Idaho National Laboratory)** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. For **Operational Technology Cybersecurity (Idaho National Laboratory)**, work from the cited evidence behind this row. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Operational Technology Cybersecurity (Idaho National Laboratory)**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must name the source descriptor, the bounded claim about **Operational Technology Cybersecurity**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape this subject work as a **cyber-physical tabletop evidence packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that Operational Technology Cybersecurity (Idaho National Laboratory) replaces human review whenever evidence looks plausible.

Transfer task. Transfer **Operational Technology Cybersecurity (Idaho National Laboratory)** to a second module by preserving safety-aware tabletop readiness and defensive coverage review, changing the source evidence, and naming a new reviewer.

63.2.3 Industrial Control Systems (ICS) and Operational Technology worked safe example: synthetic inputs, evidence, and review

Worked example: a sample water-utility tabletop reviews synthetic process logs after a simulated anomaly. [255, 2026]; [256, 2026].

Triangulation anchors. In module 45's worked-example section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **safety-aware ICS and OT intelligence**. Learners use a **cyber-physical tabletop evidence packet** and keep this boundary visible: No live device control, unsafe process change, exploit sequence, evasion, or operational response.

Frame. The classroom question centers on **ICS Architecture: SCADA, DCS, PLC, HMI — Definitions and Roles**. Excluded actions stay explicit, and the **Cyber-Physical Readiness Lens** planning question is: Which asset, architecture record, consequence, operator decision, and recovery path is being exercised defensively?

Inputs. For the **ICS Architecture: SCADA, DCS, PLC, HMI** scenario, use toy HMI screenshots, fabricated network alerts, public ICS control guidance, and a safety stop card. The Cyber-Physical Readiness Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **ICS Architecture: SCADA, DCS, PLC, HMI**, students map assets to consequences, classify tabletop injects, identify human decisions, and preserve recovery evidence. Pause whenever an inference about ICS Architecture: SCADA, DCS, PLC, HMI appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **ICS Architecture: SCADA, DCS, PLC, HMI** classroom scenario; unit artifact = cyber-physical tabletop evidence packet; evidence = allowed inputs; method = safety-aware tabletop readiness and defensive coverage review; output = a cyber-physical tabletop packet with assets, consequences, ATT&CK mapping, decisions, and debrief; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **ICS Architecture: SCADA, DCS, PLC, HMI** as "Cyber-Physical Readiness Lens confirms it" is not enough. The revision ties the claim to safety-aware tabletop readiness and defensive coverage review, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **ICS Architecture: SCADA, DCS, PLC, HMI** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

63.2.4 Industrial Control Systems (ICS) and Operational Technology practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Cyber-Physical Readiness Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition**.

Triangulation anchors. In module 45's practice-sequence section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare ICS Architecture: SCADA, DCS, PLC, HMI, SCADA: Supervisory Control and Data Acquisition, DCS: Distributed Control Systems; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane.
2. Frame	Answer the lens question: Which asset, architecture record, consequence, operator decision, and recovery path is being exercised defensively?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for ICS Architecture: SCADA, DCS, PLC, HMI: tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the cyber-physical tabletop evidence packet fields for ICS Architecture: SCADA, DCS, PLC, HMI.	Unit profile note.	Evidence artifacts include asset-consequence map, operator decision log.
4. Challenge	Test the misconception that ICS Architecture: SCADA, DCS, PLC, HMI — Definitions and Roles establishes intent without reviewing alternative explanations.	Failure-mode note.	The artifact applies the key distinction: separate cyber analysis from unsafe process control or live operational action.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

63.2.4.1 Industrial Control Systems (ICS) and Operational Technology instructor notes: source reasoning, review points, and studio focus Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition**. [255, 2026]; [256, 2026].

63.2.4.2 Industrial Control Systems (ICS) and Operational Technology extension exercise: peer validation and refresh trigger review **Evidence anchor.** Section 63; [255, 2026].

Have learners swap artifacts and apply the **Cyber-Physical Readiness Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition**.

63.2.5 Industrial Control Systems (ICS) and Operational Technology knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 63; [255, 2026].

1. Explain how **ICS Architecture: SCADA, DCS, PLC, HMI — Definitions and Roles** is defined here; name the source descriptor that supports the definition.
2. Contrast **ICS Architecture: SCADA, DCS, PLC, HMI** with **SCADA: Supervisory Control and Data Acquisition** using the **Cyber-Physical Readiness Lens** artifact fields.
3. Identify one failure mode from the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which cyber observation changes meaning once physical consequence is considered?
5. Correct this misconception: that ICS Architecture: SCADA, DCS, PLC, HMI — Definitions and Roles establishes intent without reviewing alternative explanations.

63.2.5.1 Industrial Control Systems (ICS) and Operational Technology answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **ICS Architecture: SCADA, DCS, PLC, HMI** without source evidence, uncertainty, or a safe transfer task.

63.3 Industrial Control Systems (ICS) and Operational Technology assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 63; [255, 2026].

63.3.1 Industrial Control Systems (ICS) and Operational Technology evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 63; [255, 2026].

63.3.2 Industrial Control Systems (ICS) and Operational Technology transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 63; [255, 2026].

63.3.2.1 Industrial Control Systems (ICS) and Operational Technology lineage and source tradition: profile, concepts, and first anchors This sits in the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lineage: defensive intelligence for safety-critical environments where availability, engineering state, and physical consequence matter. [255, 2026]; [256, 2026].

63.3.2.2 Industrial Control Systems (ICS) and Operational Technology working model: inputs, constraints, transforms, outputs, and oversight Evidence anchor. Section 63; [255, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition**, with provenance and reviewability throughout.

63.3.2.3 Industrial Control Systems (ICS) and Operational Technology knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** synthetic process logs, asset/consequence maps, operator decisions, safety stops, and recovery evidence. [255, 2026]; [256, 2026].
- **Transforms:** asset-consequence mapping, ATT&CK-for-ICS coverage review, operator-decision rehearsal, and after-action learning.
- **Outputs:** cyber-physical tabletop packet, debrief rubric, recovery note, and control-coverage map.
- **Failure modes:** IT-first assumptions, unsafe actuation, live-control drift, and missing safety review.

63.3.2.4 Industrial Control Systems (ICS) and Operational Technology transfer contracts: authority, evidence, tools, and auditable output Evidence anchor. Section 63; [255, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition**.
- **Evidence contract:** keep the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as cyber-physical tabletop packet, debrief rubric, recovery note, and control-coverage map that another reviewer can audit.

63.3.2.5 Industrial Control Systems (ICS) and Operational Technology profile emphasis and local focus: method stack and topic cluster Evidence anchor. Section 63; [255, 2026].

The matched profile emphasizes defensive intelligence for safety-critical environments where availability, engineering state, and physical consequence matter. The method stack is asset/consequence mapping, ATT&CK-for-ICS coverage review, defense-in-depth audit, remote-access check, and tabletop injects; the local topic cluster is **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition**.

63.3.3 Industrial Control Systems (ICS) and Operational Technology evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 63; [255, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** profile tells reviewers what evidence is strong enough for the module artifact built around **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition**.

63.3.3.1 Industrial Control Systems (ICS) and Operational Technology guide source spine: inherited keys and local citation roles Primary guide citations: [255, 2026]; [256, 2026]; [270, 2026]; [273, 2026]; [276, 2026]; [285, 2026]; [286, 2026]; [290, 2026]; [294, 2026]; [208, 2026]; [209, 2026]; [210, 2026]; [211, 2026]; [212, 2026].

63.3.3.2 Industrial Control Systems (ICS) and Operational Technology verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [255, 2026]; [256, 2026].

Tier	What counts	How it is used
Source guide	[255, 2026]; [256, 2026]; [270, 2026]; [273, 2026]; [276, 2026]; [285, 2026]; [286, 2026]; [290, 2026]; [294, 2026]; [208, 2026]; [209, 2026]; [210, 2026]; [211, 2026]; [212, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 45's source-canon section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition** and [255, 2026]; [256, 2026], but only directly verified source URLs are encoded as citations.

63.3.3.3 Industrial Control Systems (ICS) and Operational Technology intelligence practice lens: evidence artifact and safety check Practice lens: **Cyber-Physical Readiness Lens** for **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition**. [255, 2026]; [256, 2026].

Planning question: Which asset, architecture record, consequence, operator decision, and recovery path is being exercised defensively?

Evidence artifact: tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric.

Validation rule: validate against safety, availability, engineering state, incident scope, and after-action learning. Applied to **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition**.

Handoff contract: separate cyber indicators, process observations, safety impact, operator choices, and recovery evidence.

Safety check: keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions.

63.3.3.4 Industrial Control Systems (ICS) and Operational Technology runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 63; [255, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	45.99	45.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Industrial Control Systems (ICS) and Operational Technology to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Bounded autonomy, procurement, incident-response, and assurance studio	45.101	45.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Industrial Control Systems (ICS) and Operational Technology	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Model-card, recoverability, retention, and learner-support evidence package	45.102	45.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Industrial Control Systems (ICS) and Operational Technology	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
ICS Architecture: SCADA, DCS, PLC, HMI — Definitions and Roles	45.1	45.1 ICS Architecture: SCADA, DCS, PLC, HMI — Definitions and Roles	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
SCADA: Supervisory Control and Data Acquisition — Large Geographic Systems	45.1.1	45.1.1 SCADA: Supervisory Control and Data Acquisition — Large Geographic Systems	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
DCS: Distributed Control Systems — Chemical, Refining, Power	45.1.2	45.1.2 DCS: Distributed Control Systems — Chemical, Refining, Power	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
PLC: Programmable Logic Controllers — Field-Level Execution	45.1.3	45.1.3 PLC: Programmable Logic Controllers — Field-Level Execution	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
OT vs. IT: Fundamental Security Philosophy Differences	45.1.4	45.1.4 OT vs. IT: Fundamental Security Philosophy Differences	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Air-Gap Erosion: The Digital Transformation Vulnerability	45.1.5	45.1.5 Air-Gap Erosion: The Digital Transformation Vulnerability	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Securing ICS: Components, Protocols, Performance, Vulnerability	45.2	45.2 source title transformed into safe curriculum treatment; original: Securing ICS: Components, Protocols, Performance, Vulnerability	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
2026 Cybersecurity Guide to ICS (Claroty)	45.3	45.3 2026 Cybersecurity Guide to ICS (Claroty)	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
OT vs. ICS vs. SCADA Security (Palo Alto Networks)	45.4	45.4 OT vs. ICS vs. SCADA Security (Palo Alto Networks)	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Operational Technology Cybersecurity (Idaho National Laboratory)	45.5	45.5 Operational Technology Cybersecurity (Idaho National Laboratory)	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions

63.3.3.5 Industrial Control Systems (ICS) and Operational Technology reusable subsection contract: topic rows, artifacts, and safety duties Evidence anchor. Section 63; [255, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
ICS Architecture: SCADA, DCS, PLC, HMI — Definitions and Roles	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
SCADA: Supervisory Control and Data Acquisition — Large Geographic Systems	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
DCS: Distributed Control Systems — Chemical, Refining, Power	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions

Lesson topic	Practice lens	Evidence artifact	Safety check
PLC: Programmable Logic Controllers — Field-Level Execution	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
OT vs. IT: Fundamental Security Philosophy Differences	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Air-Gap Erosion: The Digital Transformation Vulnerability	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Securing ICS: Components, Protocols, Performance, Vulnerability	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
2026 Cybersecurity Guide to ICS (Claroty)	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
OT vs. ICS vs. SCADA Security (Palo Alto Networks)	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Operational Technology Cybersecurity (Idaho National Laboratory)	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions

63.3.3.6 Industrial Control Systems (ICS) and Operational Technology annotated source ledger: real titles and local contribution

Each source cited by this **ICS/OT Cyber-Physical Defense and Tabletop Readiness** module is paired below with its real title and a one-line note on what it contributes to **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition**.

Source	Cited work	What it contributes	Status
[255, 2026]	Web of Things (WoT) Architecture 1.1	The W3C Recommendation for Web of Things Architecture 1.1, published in December 2023, defining an abstract architecture for interoperability across diverse Internet of Things platforms. It introduces core concepts including Things described by machine-readable Thing Descriptions, reusable Thing Models, and Consumers that interpret descriptions to interact via Properties, Actions, and Events.	verified source-guide
[256, 2026]	Web of Things (WoT) Thing Description 1.1	The W3C WoT Thing Description 1.1 is a formal information model and standardized representation format enabling IoT devices to describe their metadata and interaction capabilities in a machine-readable way, facilitating interoperability across diverse ecosystems.	verified source-guide
[270, 2026]	NIST Big Data Interoperability Framework	NIST Special Publication 1500-1 (revised edition by Chang and Grady) establishes foundational terminology and consensus definitions for Big Data through the NIST Big Data Public Working Group. The volume defines Big Data characteristics, taxonomy, and a reference architecture assigning roles to Application Providers, Data Consumers, Data Providers, and System Orchestrators.	verified source-guide

Source	Cited work	What it contributes	Status
[273, 2026]	WCAG 2 Overview	The W3C Web Accessibility Initiative overview of the Web Content Accessibility Guidelines (WCAG), an international standard for making web content accessible to people with disabilities. It explains that WCAG is organized around four principles (perceivable, operable, understandable, robust) with testable success criteria at three conformance levels (A, AA, AAA), and covers versions 2.0, 2.1, and 2.2.	verified source-guide
[276, 2026]	What is a Data Protection Impact Assessment and When Is This Mandatory?	A European Data Protection Board FAQ page, part of its data protection guide for small businesses, explaining Data Protection Impact Assessments (DPIAs) and when they are mandatory. It describes a DPIA as a written assessment of the impact of a planned processing operation, required when processing poses high risks to individuals' rights.	verified source-guide
[285, 2026]	NIST AI Resource Center	The NIST AI Resource Center (AIRC), a government platform supporting implementation of the NIST AI Risk Management Framework, a voluntary framework for managing AI risk. It provides the core framework along with a playbook of practical actions, profiles tailored to specific sectors and technologies, use cases, and crosswalks linking the framework to other governance structures.	verified source-guide
[286, 2026]	Model Cards for Model Reporting	The arXiv abstract for "Model Cards for Model Reporting" (2018) by Mitchell, Wu, Zaldivar, and colleagues, which introduces a framework for transparent documentation of machine learning models. Model cards are short accompanying documents that report a model's benchmarked performance across varied conditions, including different cultural, demographic, and phenotypic groups, along with intended use, evaluation methodology, and deployment considerations.	verified source-guide
[290, 2026]	NIST SP 800-218A: Secure Software Development Practices for Generative AI and Dual-Use Foundation Models	NIST Special Publication 800-218A (July 2024), which augments the Secure Software Development Framework with practices specific to AI model development across the software lifecycle. Produced in response to Executive Order 14110, it addresses AI model producers, developers building on those models, and acquirers of AI systems, and is designed to be used alongside NIST SP 800-218.	verified source-guide
[294, 2026]	M-25-21: Accelerating Federal Use of AI through Innovation, Governance, and Public Trust	An April 2025 Office of Management and Budget memorandum (M-25-21) directing executive branch agencies on federal use of artificial intelligence. Issued under Executive Order 14179, it instructs agencies to accelerate adoption of AI to improve public services and government efficiency while maintaining safeguards for civil rights, civil liberties, and privacy.	verified source-guide

Source	Cited work	What it contributes	Status
[208, 2026]	Securing Industrial Control Systems: Components, Cyber Threats	This article provides a comprehensive overview of cybersecurity for Industrial Control Systems, covering SCADA, distributed control systems, and programmable logic controllers as they have evolved from isolated architectures to networked, cloud-connected deployments.	verified source-guide
[209, 2026]	What are Industrial Control Systems (ICS)? / Bitsight	A glossary entry from the cybersecurity company Bitsight explaining Industrial Control Systems (ICS), defined as integrated hardware and software used to control, monitor, and automate industrial processes across manufacturing, energy, and critical infrastructure.	verified source-guide
[210, 2026]	What Are the Differences Between OT, ICS, & SCADA Security?	A Palo Alto Networks Cyberpedia article explaining the relationship among operational technology (OT), industrial control system (ICS), and SCADA security.	verified source-guide
[211, 2026]	The 2026 Cybersecurity Guide to Industrial Control Systems - Claroty	A Claroty guide to securing industrial control systems (ICS) amid IT and operational technology convergence. It identifies challenges including an expanded attack surface, legacy systems lacking modern protections, third-party access gaps, patching delays due to uptime requirements, and advanced adversaries targeting ICS.	verified source-guide
[212, 2026]	Operational Technology Cybersecurity - Idaho National Laboratory	See bibliography for scope.	original source-guide

Where this sits. This module's overview is Section 63; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

63.3.4 Industrial Control Systems (ICS) and Operational Technology governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 63; [255, 2026].

63.3.5 Industrial Control Systems (ICS) and Operational Technology analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 45's governance-boundary section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **ICS/OT Cyber-Physical Defense and Tabletop Readiness** for **ICS Architecture: SCADA, DCS, PLC, HMI — Definitions and Roles; SCADA: Supervisory Control and Data Acquisition — Large Geographic Systems**. [255, 2026]; [256, 2026].

Curriculum topic spine: ICS Architecture: SCADA, DCS, PLC, HMI — Definitions and Roles, **SCADA: Supervisory Control and Data Acquisition — Large Geographic Systems**, **DCS: Distributed Control Systems — Chemical, Refining, Power**. **Verified anchor cluster:** [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]; [Cybersecurity and Agency, 2026a]; [Cybersecurity and Agency, 2026c]; [MITRE, 2026c].

Conceptual depth: defensive intelligence for safety-critical environments where availability, engineering state, and physical consequence matter.

Method stack: asset/consequence mapping, ATT&CK-for-ICS coverage review, defense-in-depth audit, remote-access check, and tabletop injects.

Composability contract: separate cyber indicators, engineering observations, safety impacts, operator decisions, and recovery actions.

Known failure modes: IT-first assumptions, unsafe automation, untested shutdown logic, poor remote-access control, and missing after-action learning.

Defensive boundary: all ICS work remains tabletop, lab, or accountable defensive review; no exploitation, unsafe process manipulation, or live control actions. Applied to **ICS Architecture: SCADA, DCS, PLC, HMI — Definitions and Roles; SCADA: Supervisory Control and Data Acquisition — Large Geographic Systems**.

Anchor	Why it matters here
[of Standards and Technology, 2024f]	Official cybersecurity-risk governance framework that adds the Govern function and supplies a common language for AI, OT, and enterprise risk. Checked as of 2026-05-21; role: curriculum_anchor.
[of Standards and Technology, 2022b]	Systems-security engineering foundation for trustworthy systems in contested operational environments and related training programs. Checked as of 2026-05-21; role: curriculum_anchor.
[of Standards and Technology, 2024b]	Official NIST operational technology security guidance. Checked as of 2026-05-21; role: source_quality_anchor.
[of Automation, 2026]	Official ISA overview of industrial automation and control security standards. Checked as of 2026-05-21; role: source_quality_anchor.
[Cybersecurity and Agency, 2026a]	Official prioritized baseline of IT and OT cybersecurity practices for critical-infrastructure risk reduction and maturity assessment. Checked as of 2026-05-21; role: curriculum_anchor.
[Cybersecurity and Agency, 2026c]	Official defensive ICS practice library for defense-in-depth, forensics, incident response, and remote access. Checked as of 2026-05-21; role: curriculum_anchor.
[MITRE, 2026c]	Threat-informed defensive matrix for ICS tactics and techniques, used for coverage mapping. Checked as of 2026-05-21; role: curriculum_anchor.

63.3.5.1 Industrial Control Systems (ICS) and Operational Technology evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [255, 2026]; [256, 2026].

63.3.6 Industrial Control Systems (ICS) and Operational Technology agentic boundary: assist, approve, block, and record

Evidence anchor. Section 63; [255, 2026].

AGEINT translation is bounded by the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition**.

63.3.6.1 Industrial Control Systems (ICS) and Operational Technology permitted defensive utility: curriculum uses and safe outputs

Evidence anchor. Section 63; [255, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition**.

63.3.6.2 Industrial Control Systems (ICS) and Operational Technology excluded operational boundary: blocked actions and stop rules

Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [255, 2026]; [256, 2026] and **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

63.3.7 Industrial Control Systems (ICS) and Operational Technology governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 63; [255, 2026].

Governance is practiced as a gate on the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane. Learners use the **Cyber-Physical Readiness Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition**.

63.3.7.1 Industrial Control Systems (ICS) and Operational Technology governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [255, 2026]; [256, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **ICS/OT Cyber-Physical Defense and Tabletop Readiness** failure modes and the **Cyber-Physical Readiness Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

63.3.7.2 Industrial Control Systems (ICS) and Operational Technology evidence package handoff: appendices, records, and reuse Evidence anchor. Section 63; [255, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Cyber-Physical Readiness Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition**.

63.3.7.3 Industrial Control Systems (ICS) and Operational Technology current-source assurance: verified anchors and local artifact fit The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition**. [255, 2026]; [256, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_nist_csf_2` for **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition**?	The NIST Cybersecurity Framework (CSF) 2.0; lane `ics_ot_defense`; checked 2026-05-21.	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric; Official cybersecurity-risk governance framework that adds the Govern function and supplies a common language for AI, OT, and enterprise risk.
What does the module inherit from `official_nist_sp_800_160r1` for **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition**?	Engineering Trustworthy Secure Systems, NIST SP 800-160 Vol. 1 Rev. 1; lane `ics_ot_defense`; checked 2026-05-21.	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric; Systems-security engineering foundation for trustworthy systems in contested operational environments and related training programs.
What does the module inherit from `official_nist_sp_800_82r3` for **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition**?	Guide to Operational Technology Security, NIST SP 800-82 Rev. 3; lane `source_quality_spine`; checked 2026-05-21.	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric; Official NIST operational technology security guidance.
What does the module inherit from `official_isa_iec_62443` for **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition**?	ISA/IEC 62443 Series of Standards; lane `source_quality_spine`; checked 2026-05-21.	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric; Official ISA overview of industrial automation and control security standards.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 63; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

63.3.8 Industrial Control Systems (ICS) and Operational Technology assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 63; [255, 2026].

63.3.9 Industrial Control Systems (ICS) and Operational Technology assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 63; [255, 2026].

63.3.9.1 Industrial Control Systems (ICS) and Operational Technology capstone pathway: reviewable packet and excluded use

The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition** and [255, 2026]; [256, 2026].

63.3.9.2 Industrial Control Systems (ICS) and Operational Technology instructor facilitation notes: studio roles and pause points

Facilitate as a bounded studio around **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition** and [255, 2026]; [256, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

63.3.9.3 Industrial Control Systems (ICS) and Operational Technology assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
ICS Architecture: SCADA, DCS, PLC, HMI — Definitions and Roles	Completed **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
SCADA: Supervisory Control and Data Acquisition — Large Geographic Systems	Completed **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
DCS: Distributed Control Systems — Chemical, Refining, Power	Completed **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

63.3.10 Industrial Control Systems (ICS) and Operational Technology refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [255, 2026]; [256, 2026] and **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition**.

63.3.10.1 Industrial Control Systems (ICS) and Operational Technology refresh triggers: source changes and required actions

Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition**. The local signals begin with [255, 2026]; [256, 2026].

63.3.10.2 Industrial Control Systems (ICS) and Operational Technology claim and evidence ledger: claim classes, caveats, and owners

The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition**, and the source spine for these checks begins with [255, 2026]; [256, 2026].

63.3.11 Industrial Control Systems (ICS) and Operational Technology reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [255, 2026]; [256, 2026].

Triangulation anchors. In module 45's review-checklist section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition**. [255, 2026]; [256, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.

- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

63.3.12 Industrial Control Systems (ICS) and Operational Technology learning-path links: module map, overview, and curriculum atlas

Use the cross-links below to place **ICS Architecture: SCADA, DCS, PLC, HMI; SCADA: Supervisory Control and Data Acquisition** in the wider unit: the orientation sets the frame, the parent unit supplies the shared safety posture, and the neighbouring modules show what evidence enters and leaves. Lead sources: [255, 2026]; [256, 2026].
Section 2, Section 62, Section 64

64 MITRE ATT&CK for ICS

64.0.1 MITRE ATT&CK for ICS figures and course links: visual evidence, source flow, and navigation

The module uses Figure 138 and Figure 134 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.

Navigation links: Section 2, Section 62, Section 63, Section 65.

This module teaches the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane through a bounded, source-backed coursebook chapter. [255, 2026]; [257, 2026].

64.1 ICS/OT Cyber-Physical Defense and Tabletop Readiness frame for MITRE ATT&CK for ICS: source context, topic focus, and reader task

Evidence anchor. Section 64; [255, 2026].

64.1.1 MITRE ATT&CK for ICS orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 64; [255, 2026].

64.1.2 MITRE ATT&CK for ICS conceptual primer: source context, core model, and reader task

This chapter teaches ICS/OT intelligence as safety-aware defensive reasoning: asset state, engineering consequence, operator decision, and recovery evidence matter as much as cyber indicators. The chapter uses **Cyber-Physical Readiness Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**.

The central distinction is to separate cyber analysis from unsafe process control or live operational action. Core topics include **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts; ICS controller-change coverage review using synthetic process records**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.

Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [255, 2026]; [257, 2026].

Learners move from vocabulary and the **Cyber-Physical Readiness Lens** distinction through topic lessons on **ICS Matrix: 12 Tactics, Full Technique Library** with evidence and misconception checks, then assemble a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** with safety and rights gates.

64.1.3 MITRE ATT&CK for ICS learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 64; [255, 2026].

- Connect **ICS Matrix: 12 Tactics, Full Technique Library and Cyber access-and-execution taxonomy review using fabricated alerts** to **ICS/OT Cyber-Physical Defense and Tabletop Readiness** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate cyber analysis from unsafe process control or live operational action; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as IT-first assumptions, unsafe automation, untested shutdown logic, poor remote-access control, and missing after-action learning, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: all ICS work remains tabletop, lab, or accountable defensive review; no exploitation, unsafe process manipulation, or live control actions.

64.1.4 MITRE ATT&CK for ICS core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 64; [255, 2026].

Term	Working definition
Engineering state	the physical or process condition that gives cyber evidence safety meaning
Consequence	the operational, safety, environmental, or service effect of a condition
Defense in depth	layered prevention, detection, response, and recovery controls
Tabletop inject	a synthetic event used to rehearse decisions without touching live systems
Recovery evidence	proof that a safe state, service, or learning objective was restored
ICS Matrix: 12 Tactics, Full Technique Library	Key terms: ICS, Matrix, Tactics.
Cyber access-and-execution taxonomy review…	Key terms: Cyber, access, execution.

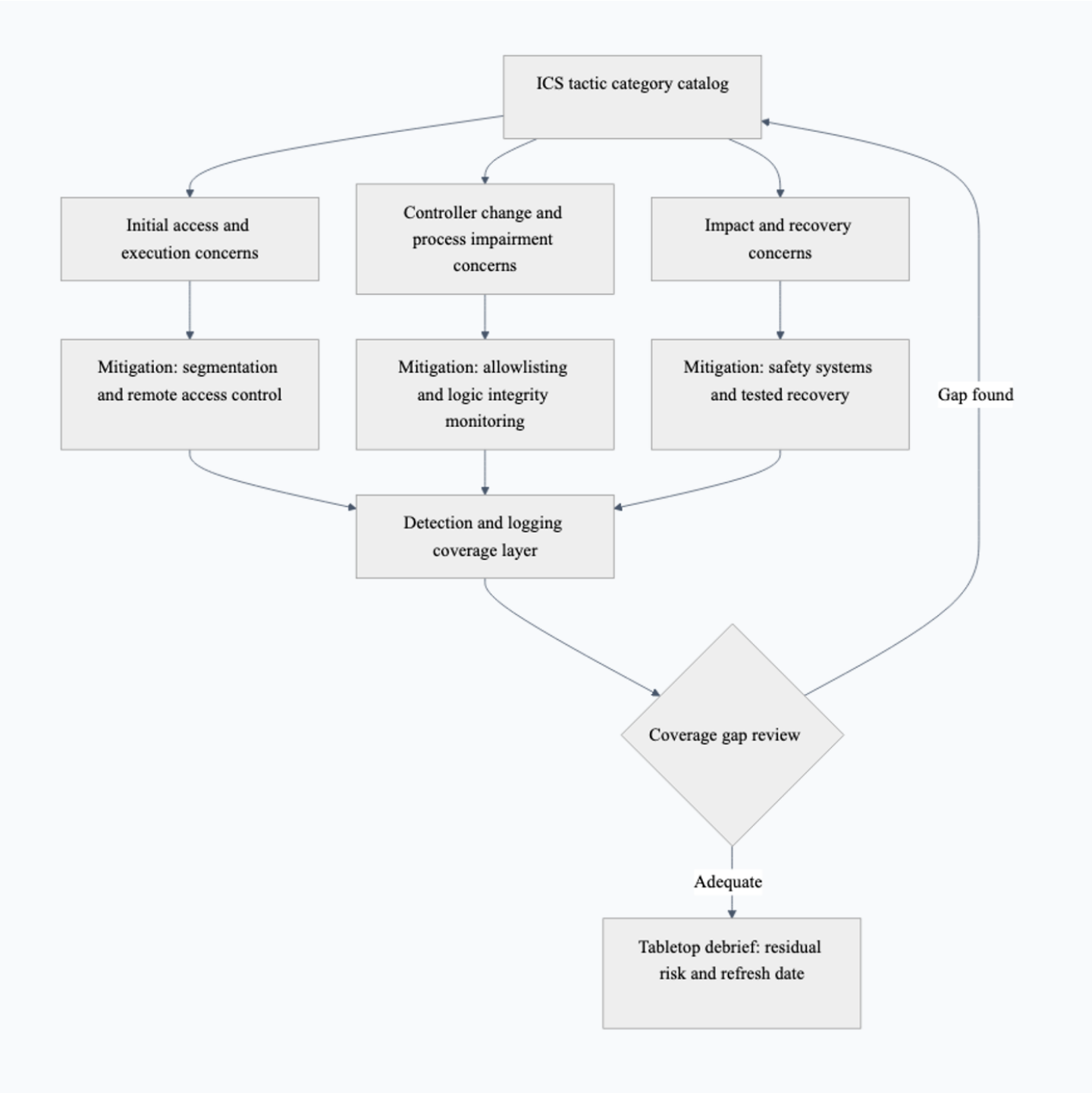


Figure 138: A defensive coverage view that maps adversary tactic categories in the ICS matrix to layered mitigations and detection so a tabletop team can find gaps. In the industrial and cyber physical intelligence / mitre att ck for ics section, it lets readers compare ICS tactic category catalog, Initial access and execution concerns, Controller change and process impairment concerns, and Impact and recovery concerns so the visual functions as a traceable course aid rather than an unscoped assertion.

64.2 Cyber-Physical Readiness Lens path for MITRE ATT&CK for ICS: lesson cluster, safe artifact, and review

Evidence anchor. Section 64; [255, 2026].

64.2.1 MITRE ATT&CK for ICS practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 64; [255, 2026].

64.2.2 MITRE ATT&CK for ICS topic lessons: source-backed concepts and transfer tasks

This module builds ICS/OT intelligence as safety-aware defensive reasoning: asset state, engineering consequence, operator decision, and recovery evidence matter as much as cyber indicators. The sequence opens with **ICS Matrix: 12 Tactics, Full Technique Library**, **Cyber access-and-execution taxonomy review using fabricated alerts**, **ICS controller-change coverage review using synthetic process records** and applies the **Cyber-Physical Readiness Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 134; module overview Section 64; curriculum atlas Section 2.

Triangulation anchors. In module 46's topic-lessons section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

64.2.2.1 Lesson 1: ICS Matrix: 12 Tactics, Full Technique Library

Concept. ICS Matrix: 12 Tactics, Full Technique Library applies ICS, Matrix, Tactics within ICS/OT Cyber-Physical Defense and Tabletop Readiness: learners use separate cyber analysis from unsafe process control or live operational action and safety-aware tabletop readiness and defensive coverage review evidence before any judgment moves forward.

Why it matters. Without explicit treatment of **ICS Matrix: 12 Tactics, Full Technique Library**, IT-first assumptions undermines safety-aware tabletop readiness and defensive coverage review; the lesson builds the habit to separate cyber analysis from unsafe process control or live operational action.

Source support. ICS Matrix: 12 Tactics, Full Technique Library rests on [213, 2026]. The lead source's own note reads: The matrix organizes methods into twelve tactical categories spanning initial access through impact, including ICS-specific concerns such as firmware modification and disruption of operational technology. Use it for pinning down the scope of **ICS Matrix: 12 Tactics, Full Technique Library**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. Read **ICS Matrix: 12 Tactics, Full Technique Library** against the works cited for this row. [213, 2026] The Industrial Control Systems (ICS) domain of the MITRE ATT&CK framework, a knowledge base documenting adversary behaviors based on real-world observations of attacks on critical infrastructure. The matrix organizes methods into twelve tactical categories spanning initial access through impact, including ICS-specific concerns such as firmware modification and disruption of operational technology. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **ICS Matrix**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must name the source descriptor, the bounded claim about **ICS Matrix**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **ICS Matrix: 12 Tactics, Full Technique Library** work as a **cyber-physical tabletop evidence packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that ICS Matrix: 12 Tactics, Full Technique Library is optional whenever separate cyber analysis from unsafe process control or live operational action feels inconvenient.

Transfer task. Transfer **ICS Matrix: 12 Tactics, Full Technique Library** to a second module by preserving safety-aware tabletop readiness and defensive coverage review, changing the source evidence, and naming a new reviewer.

64.2.2.2 Lesson 2: Cyber access-and-execution taxonomy review using fabricated alerts

Concept. Cyber access-and-execution taxonomy review using fabricated alerts uses the taxonomy label to organize fabricated defensive observations, confidence, and control implications without describing adversary execution.

Why it matters. Cyber access-and-execution taxonomy review connects classroom vocabulary to ICS/OT Cyber-Physical Defense and Tabletop Readiness practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Cyber access-and-execution taxonomy review using fabricated alerts rests on [213, 2026]. The most specific cited work observes: The Industrial Control Systems (ICS) domain of the MITRE ATT&CK framework, a knowledge base documenting adversary behaviors based on real-world observations of attacks on critical infrastructure. Use it for fixing what **Cyber access-and-execution taxonomy review using fabricated alerts** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. For **Cyber access-and-execution taxonomy review**, reason from the sources cited in this row. [213, 2026] The Industrial Control Systems (ICS) domain of the MITRE ATT&CK framework, a knowledge base documenting adversary behaviors based on real-world observations of attacks on critical infrastructure. The matrix organizes methods into twelve tactical categories spanning initial access through impact, including ICS-specific concerns such as firmware modification and disruption of operational technology. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Cyber access-and-execution taxonomy review**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must map the indicator descriptor, the bounded claim about **Cyber access-and-execution taxonomy review using**, the taxonomy caveat, the confidence note, the no-action boundary, and the reviewer who validates the labeling. Shape **Cyber access-and-execution taxonomy review** work as a **cyber-physical tabletop evidence packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Cyber access-and-execution taxonomy review**: that a defensive taxonomy label is an action sequence rather than a vocabulary for describing and detecting behavior.

Transfer task. Reuse the **Cyber access-and-execution taxonomy review** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

64.2.2.3 Lesson 3: ICS controller-change coverage review using synthetic process records

Concept. ICS controller-change coverage review using synthetic process records maps requirements to collection gaps, priorities, and reviewer sign-off.

Why it matters. Analysts use **ICS controller-change coverage review** to separate cyber analysis from unsafe process control or live operational action. A defensible treatment names the judgment it enables for safety-aware tabletop readiness and defensive coverage review, the proof limit that IT-first assumptions would otherwise hide, and the reviewer accountable for challenge.

Source support. ICS controller-change coverage review using synthetic process records rests on [213, 2026]. The lead source's own note reads: The matrix organizes methods into twelve tactical categories spanning initial access through impact, including ICS-specific concerns such as firmware modification and disruption of operational technology. Use it for pinning down the scope of **ICS controller-change coverage review**

using synthetic process records, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. Ground **ICS controller-change coverage review** in the evidence the row cites. [213, 2026] The Industrial Control Systems (ICS) domain of the MITRE ATT&CK framework, a knowledge base documenting adversary behaviors based on real-world observations of attacks on critical infrastructure. The matrix organizes methods into twelve tactical categories spanning initial access through impact, including ICS-specific concerns such as firmware modification and disruption of operational technology. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **ICS controller-change coverage review**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must list the asset descriptor, the bounded claim about **ICS controller-change coverage review using**, the safety caveat, the uncertainty note, the no-live-actuation boundary, and the reviewer who owns the safety case. Shape **ICS controller-change coverage review** work as a **cyber-physical tabletop evidence packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **ICS controller-change coverage review**: that an industrial control system behaving normally proves it is safe, rather than a state that depends on intact safeguards and monitoring.

Transfer task. Apply this module's safe boundary for **ICS controller-change coverage review** to another artifact while keeping safety-aware tabletop readiness and defensive coverage review and reviewer ownership explicit.

64.2.2.4 Lesson 4: ICS firmware and project-integrity coverage

Concept. ICS firmware and project-integrity coverage translates the technique family into safety, availability, operator decision, and recovery-evidence questions for a tabletop.

Why it matters. ICS firmware and project-integrity coverage connects classroom vocabulary to ICS/OT Cyber-Physical Defense and Tabletop Readiness practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. ICS firmware and project-integrity coverage rests on [213, 2026]. Its anchor reference records: The Industrial Control Systems (ICS) domain of the MITRE ATT&CK framework, a knowledge base documenting adversary behaviors based on real-world observations of attacks on critical infrastructure. Use it for fixing what **ICS firmware and project-integrity coverage** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. Read **ICS firmware and project-integrity coverage** against the works cited for this row. [213, 2026] The Industrial Control Systems (ICS) domain of the MITRE ATT&CK framework, a knowledge base documenting adversary behaviors based on real-world observations of attacks on critical infrastructure. The matrix organizes methods into twelve tactical categories spanning initial access through impact, including ICS-specific concerns such as firmware modification and disruption of operational technology. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. Build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must list the asset descriptor, the bounded claim about **ICS firmware and project-integrity coverage**, the safety caveat, the uncertainty note, the no-live-actuation boundary, and the reviewer who owns the safety case. Shape this subject work as a **cyber-physical tabletop evidence packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **ICS firmware and project-integrity coverage**: that an industrial control system behaving normally proves it is safe, rather than a state that depends on intact safeguards and monitoring.

Transfer task. Reuse the **ICS firmware and project-integrity coverage** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

64.2.2.5 Lesson 5: ICS evasion coverage-control review using defensive detection questions

Concept. ICS evasion coverage-control review using defensive detection questions uses the tactic family as a defensive coverage question: which monitoring, logging, and operator-review controls would reveal evasion in a tabletop scenario?

Why it matters. Analysts use **ICS evasion coverage-control review** to separate cyber analysis from unsafe process control or live operational action. A defensible treatment names the judgment it enables for safety-aware tabletop readiness and defensive coverage review, the proof limit that IT-first assumptions would otherwise hide, and the reviewer accountable for challenge.

Source support. ICS evasion coverage-control review using defensive detection questions rests on [213, 2026]. Its anchor reference records: The matrix organizes methods into twelve tactical categories spanning initial access through impact, including ICS-specific concerns such as firmware modification and disruption of operational technology. Use it for the claim that **ICS evasion coverage-control review using defensive detection questions** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. Read **ICS evasion coverage-control review** against the works cited for this row. [213, 2026] The Industrial Control Systems (ICS) domain of the MITRE ATT&CK framework, a knowledge base documenting adversary behaviors based on real-world observations of attacks on critical infrastructure. The matrix organizes methods into twelve tactical categories spanning initial access through impact, including ICS-specific concerns such as firmware modification and disruption of operational technology. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **ICS evasion coverage-control review**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must list the coverage descriptor, the bounded claim about **ICS evasion coverage-control review using**, the detection-gap caveat, the uncertainty note, the no-evasion boundary, and the reviewer who owns the control review. Shape **ICS evasion coverage-control review** work as a **cyber-physical tabletop evidence packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that mapping how detection can be evaded in control systems is a how-to, rather than a defensive map of where monitoring coverage must be hardened.

Transfer task. Transfer **ICS evasion coverage-control review** from this module to a second motif by preserving safety-aware tabletop readiness and defensive coverage review, replacing action with audit, and naming the blocked use.

64.2.2.6 Lesson 6: ICS defensive coverage and safety tabletop using synthetic process records

Concept. ICS defensive coverage and safety tabletop using synthetic process records translates the technique family into safety, availability, operator decision, and recovery-evidence questions for a tabletop.

Why it matters. ICS defensive coverage connects classroom vocabulary to ICS/OT Cyber-Physical Defense and Tabletop Readiness practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. ICS defensive coverage and safety tabletop using synthetic process records rests on [213, 2026]. The most specific cited work observes: The matrix organizes methods into twelve tactical categories spanning initial access through impact, including ICS-specific concerns such as firmware modification and disruption of operational technology. Use it for the claim that **ICS defensive coverage and safety tabletop using synthetic process records** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. For **ICS defensive coverage**, reason from the sources cited in this row. [213, 2026] The Industrial Control Systems (ICS) domain of the MITRE ATT&CK framework, a knowledge base documenting adversary behaviors based on real-world observations of attacks on critical

infrastructure. The matrix organizes methods into twelve tactical categories spanning initial access through impact, including ICS-specific concerns such as firmware modification and disruption of operational technology. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **ICS defensive coverage**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must list the asset descriptor, the bounded claim about **ICS defensive coverage and safety**, the safety caveat, the uncertainty note, the no-live-actuation boundary, and the reviewer who owns the safety case. Shape **ICS defensive coverage** work as a **cyber-physical tabletop evidence packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **ICS defensive coverage**: that an industrial control system behaving normally proves it is safe, rather than a state that depends on intact safeguards and monitoring.

Transfer task. Transfer **ICS defensive coverage** from this module to a second motif by preserving safety-aware tabletop readiness and defensive coverage review, replacing action with audit, and naming the blocked use.

64.2.2.7 Lesson 7: Cyber credential-and-movement taxonomy review using fabricated alerts

Concept. Cyber credential-and-movement taxonomy review using fabricated alerts uses the taxonomy label to organize fabricated defensive observations, confidence, and control implications without describing adversary execution.

Why it matters. Analysts use **Cyber credential-and-movement taxonomy review** to separate cyber analysis from unsafe process control or live operational action. A defensible treatment names the judgment it enables for safety-aware tabletop readiness and defensive coverage review, the proof limit that treating defensive taxonomy labels as an action sequence would otherwise hide, and the reviewer accountable for challenge.

Source support. Cyber credential-and-movement taxonomy review using fabricated alerts rests on [213, 2026]. Its anchor reference records: The matrix organizes methods into twelve tactical categories spanning initial access through impact, including ICS-specific concerns such as firmware modification and disruption of operational technology. Use it for fixing what **Cyber credential-and-movement taxonomy review using fabricated alerts** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. Read **Cyber credential-and-movement taxonomy review** against the works cited for this row. [213, 2026] The Industrial Control Systems (ICS) domain of the MITRE ATT&CK framework, a knowledge base documenting adversary behaviors based on real-world observations of attacks on critical infrastructure. The matrix organizes methods into twelve tactical categories spanning initial access through impact, including ICS-specific concerns such as firmware modification and disruption of operational technology. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Cyber credential-and-movement taxonomy review**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must map the indicator descriptor, the bounded claim about **Cyber credential-and-movement taxonomy review using**, the taxonomy caveat, the confidence note, the no-action boundary, and the reviewer who validates the labeling. Shape **Cyber credential-and-movement taxonomy review** work as a **cyber-physical tabletop evidence packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Cyber credential-and-movement taxonomy review**: that a defensive taxonomy label is an action sequence rather than a vocabulary for describing and detecting behavior.

Transfer task. Reuse the **Cyber credential-and-movement taxonomy review** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

64.2.2.8 Lesson 8: ICS collection-risk detection review using synthetic tag records

Concept. ICS collection-risk detection review using synthetic tag records uses the tactic family as a detection-design question over synthetic process tags, not as guidance for observing or changing a real process.

Why it matters. Analysts use **ICS collection-risk detection review** to separate cyber analysis from unsafe process control or live operational action. A defensible treatment names the judgment it enables for safety-aware tabletop readiness and defensive coverage review, the proof limit that IT-first assumptions would otherwise hide, and the reviewer accountable for challenge.

Source support. ICS collection-risk detection review using synthetic tag records rests on [213, 2026]. The most specific cited work observes: The Industrial Control Systems (ICS) domain of the MITRE ATT&CK framework, a knowledge base documenting adversary behaviors based on real-world observations of attacks on critical infrastructure. Use it for fixing what **ICS collection-risk detection review using synthetic tag records** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. For **ICS collection-risk detection review**, work from the cited evidence behind this row. [213, 2026] The Industrial Control Systems (ICS) domain of the MITRE ATT&CK framework, a knowledge base documenting adversary behaviors based on real-world observations of attacks on critical infrastructure. The matrix organizes methods into twelve tactical categories spanning initial access through impact, including ICS-specific concerns such as firmware modification and disruption of operational technology. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **ICS collection-risk detection review**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must list the observation descriptor, the bounded claim about **ICS collection-risk detection review using**, the detection caveat, the uncertainty note, the approved-point boundary, and the reviewer who validates coverage. Shape **ICS collection-risk detection review** work as a **cyber-physical tabletop evidence packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that describing how collection against control systems is detected is an evasion guide, rather than knowledge for strengthening detection.

Transfer task. Transfer **ICS collection-risk detection review** from this module to a second motif by preserving safety-aware tabletop readiness and defensive coverage review, replacing action with audit, and naming the blocked use.

64.2.2.9 Lesson 9: ICS alarm and communications-resilience tabletop

Concept. ICS alarm and communications-resilience tabletop translates the technique family into safety, availability, operator decision, and recovery-evidence questions for a tabletop.

Why it matters. ICS alarm and communications-resilience tabletop matters in the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane because safety-aware tabletop readiness and defensive coverage evidence must stay separate from judgment; IT-first assumptions is a common failure.

Source support. ICS alarm and communications-resilience tabletop rests on [213, 2026]. The closest source to this row notes: The matrix organizes methods into twelve tactical categories spanning initial access through impact, including ICS-specific concerns such as firmware modification and disruption of operational technology. Use it for pinning down the scope of **ICS alarm and communications-resilience tabletop**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. For **ICS alarm and communications-resilience tabletop**, reason from the sources cited in this row. [213, 2026] The Industrial Control Systems (ICS) domain of the MITRE ATT&CK framework, a knowledge base documenting adversary behaviors based on real-world observations of attacks on critical infrastructure. The matrix organizes methods into twelve tactical categories spanning initial access through impact,

including ICS-specific concerns such as firmware modification and disruption of operational technology. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. Build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must list the asset descriptor, the bounded claim about **ICS alarm and communications-resilience tabletop**, the safety caveat, the uncertainty note, the no-live-actuation boundary, and the reviewer who owns the safety case. Shape this subject work as a **cyber-physical tabletop evidence packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **ICS alarm and communications-resilience tabletop**: that an industrial control system behaving normally proves it is safe, rather than a state that depends on intact safeguards and monitoring.

Transfer task. Transfer **ICS alarm and communications-resilience tabletop** from this module to a second motif by preserving safety-aware tabletop readiness and defensive coverage review, replacing action with audit, and naming the blocked use.

64.2.2.10 Lesson 10: ICS process-safety consequence review using synthetic records Concept. ICS process-safety consequence review using synthetic records translates the technique family into safety, availability, operator decision, and recovery-evidence questions for a tabletop.

Why it matters. ICS process-safety consequence review connects classroom vocabulary to ICS/OT Cyber-Physical Defense and Tabletop Readiness practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. ICS process-safety consequence review using synthetic records rests on [213, 2026]. The most specific cited work observes: The matrix organizes methods into twelve tactical categories spanning initial access through impact, including ICS-specific concerns such as firmware modification and disruption of operational technology. Use it for fixing what **ICS process-safety consequence review using synthetic records** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. Read **ICS process-safety consequence review** against the works cited for this row. [213, 2026] The Industrial Control Systems (ICS) domain of the MITRE ATT&CK framework, a knowledge base documenting adversary behaviors based on real-world observations of attacks on critical infrastructure. The matrix organizes methods into twelve tactical categories spanning initial access through impact, including ICS-specific concerns such as firmware modification and disruption of operational technology. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **ICS process-safety consequence review**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must list the asset descriptor, the bounded claim about **ICS process-safety consequence review using**, the safety caveat, the uncertainty note, the no-live-actuation boundary, and the reviewer who owns the safety case. Shape **ICS process-safety consequence review** work as a **cyber-physical tabletop evidence packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **ICS process-safety consequence review**: that an industrial control system behaving normally proves it is safe, rather than a state that depends on intact safeguards and monitoring.

Transfer task. Transfer **ICS process-safety consequence review** from this module to a second motif by preserving safety-aware tabletop readiness and defensive coverage review, replacing action with audit, and naming the blocked use.

64.2.2.11 Lesson 11: Impact: ICS defensive coverage and safety tabletop using synthetic process records Concept. Impact: ICS defensive coverage and safety tabletop using synthetic process records translates the technique family into safety, availability, operator decision, and recovery-evidence questions for a tabletop.

Why it matters. Impact: ICS defensive coverage and safety tabletop using synthetic process records matters in the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane because safety-aware tabletop readiness and defensive coverage evidence must stay separate from judgment; IT-first assumptions is a common failure.

Source support. Impact: ICS defensive coverage and safety tabletop using synthetic process records rests on [213, 2026]. Its anchor reference records: The matrix organizes methods into twelve tactical categories spanning initial access through impact, including ICS-specific concerns such as firmware modification and disruption of operational technology. Use it for fixing what **Impact: ICS defensive coverage and safety tabletop using synthetic process records** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. Read **Impact: ICS defensive coverage and safety tabletop using synthetic process records** against the works cited for this row. [213, 2026] The Industrial Control Systems (ICS) domain of the MITRE ATT&CK framework, a knowledge base documenting adversary behaviors based on real-world observations of attacks on critical infrastructure. The matrix organizes methods into twelve tactical categories spanning initial access through impact, including ICS-specific concerns such as firmware modification and disruption of operational technology. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Impact**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must list the asset descriptor, the bounded claim about **Impact**, the safety caveat, the uncertainty note, the no-live-actuation boundary, and the reviewer who owns the safety case. Shape **Impact: ICS defensive coverage and safety tabletop using synthetic process records** work as a **cyber-physical tabletop evidence packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Impact: ICS defensive coverage and safety tabletop using synthetic process records**: that an industrial control system behaving normally proves it is safe, rather than a state that depends on intact safeguards and monitoring.

Transfer task. Apply this module's safe boundary for **Impact: ICS defensive coverage and safety tabletop using synthetic process records** to another artifact while keeping safety-aware tabletop readiness and defensive coverage review and reviewer ownership explicit.

64.2.2.12 Lesson 12: Using ICS ATT&CK in Risk Assessment (ISA InTech) Concept. Using ICS ATT&CK in Risk Assessment (ISA InTech) applies ICS, ATT, CK within ICS/OT Cyber-Physical Defense and Tabletop Readiness: learners use separate cyber analysis from unsafe process control or live operational action and safety-aware tabletop readiness and defensive coverage review evidence before any judgment moves forward.

Why it matters. Without explicit treatment of **Using ICS ATT&CK in Risk Assessment (ISA InTech)**, IT-first assumptions undermines safety-aware tabletop readiness and defensive coverage review; the lesson builds the habit to separate cyber analysis from unsafe process control or live operational action.

Source support. Using ICS ATT&CK in Risk Assessment (ISA InTech) rests on [214, 2026]. The lead source's own note reads: A June 2021 InTech Magazine article by Jacob Chapman, published by the International Society of Automation, on using the ICS ATT&CK framework to strengthen cybersecurity for manufacturing and industrial IoT systems. Use it for the working definition that **Using ICS ATT&CK in Risk Assessment (ISA InTech)** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. For **Using ICS ATT&CK in Risk Assessment (ISA InTech)**, reason from the sources cited in this row. [214, 2026] A June 2021 InTech Magazine article by Jacob Chapman, published by the International Society of Automation, on using the ICS ATT&CK framework to strengthen cybersecurity for manufacturing and industrial IoT systems. It describes a three-phase risk-management approach: gathering information

on assets and network architecture, mapping potential attack paths to identify vulnerabilities, and prioritizing mitigations by impact. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Using ICS ATT&CK**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must name the source descriptor, the bounded claim about **Using ICS ATT&CK in Risk**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Using ICS ATT&CK in Risk Assessment (ISA InTech)** work as a **cyber-physical tabletop evidence packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that Using ICS ATT&CK in Risk Assessment (ISA InTech) can be used while ignoring the rule to separate cyber analysis from unsafe process control or live operational action.

Transfer task. Transfer **Using ICS ATT&CK in Risk Assessment (ISA InTech)** to a second module by preserving safety-aware tabletop readiness and defensive coverage review, changing the source evidence, and naming a new reviewer.

64.2.2.13 Lesson 13: Dragos: MITRE ATT&CK for ICS Threat Actor Mapping

Concept. Dragos: MITRE ATT&CK for ICS Threat Actor Mapping uses ATT&CK for ICS as defensive vocabulary for sequencing observations over synthetic process records—not adversary execution.

Why it matters. Analysts use **Dragos: MITRE ATT&CK for ICS Threat Actor Mapping** to separate cyber analysis from unsafe process control or live operational action. A defensible treatment names the judgment it enables for safety-aware tabletop readiness and defensive coverage review, the proof limit that IT-first assumptions would otherwise hide, and the reviewer accountable for challenge.

Source support. Dragos: MITRE ATT&CK for ICS Threat Actor Mapping rests on [215, 2026]. The lead source's own note reads: It explains how the Dragos Platform maps detections to ATT&CK tactics and techniques through regular knowledge updates, profiles named threat groups, and organizes behaviors across tactic areas spanning initial access through impact scenarios such as loss of control, safety, or availability. Use it for fixing what **Dragos: MITRE ATT&CK for ICS Threat Actor Mapping** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. For **Dragos: MITRE ATT&CK for ICS Threat Actor Mapping**, work from the cited evidence behind this row. [215, 2026] A Dragos solutions page describing the module framework, a knowledge base of adversary behaviors observed in attacks against industrial control system networks. It explains how the Dragos Platform maps detections to ATT&CK tactics and techniques through regular knowledge updates, profiles named threat groups, and organizes behaviors across tactic areas spanning initial access through impact scenarios such as loss of control, safety, or availability. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Dragos**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must name the source descriptor, the bounded claim about **Dragos**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Dragos: MITRE ATT&CK for ICS Threat Actor Mapping** work as a **cyber-physical tabletop evidence packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that Dragos: the module Threat Actor Mapping is optional whenever separate cyber analysis from unsafe process control or live operational action feels inconvenient.

Transfer task. Transfer **Dragos: MITRE ATT&CK for ICS Threat Actor Mapping** to a second module by preserving safety-aware tabletop readiness and defensive coverage review, changing the source evidence, and naming a new reviewer.

64.2.2.14 Lesson 14: Nozomi Networks: How Security Teams Use the ICS Framework

Concept. Nozomi Networks: How Security Teams Use the ICS Framework applies Nozomi, Networks, How within ICS/OT Cyber-Physical Defense and Tabletop Readiness: learners use separate cyber analysis from unsafe process control or live operational action and safety-aware tabletop readiness and defensive coverage review evidence before any judgment moves forward.

Why it matters. Without explicit treatment of **Nozomi Networks**, IT-first assumptions undermines safety-aware tabletop readiness and defensive coverage review; the lesson builds the habit to separate cyber analysis from unsafe process control or live operational action.

Source support. Nozomi Networks: How Security Teams Use the ICS Framework rests on [216, 2026]. The most specific cited work observes: It explains that the ICS version is a community-sourced knowledge base mapping adversary tactics and behaviors specific to industrial environments, distinct from the IT-focused framework. Use it for the working definition that **Nozomi Networks: How Security Teams Use the ICS Framework** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. Ground **Nozomi Networks** in the evidence the row cites. [216, 2026] A Nozomi Networks resource (a 2020 webinar) on how security teams apply the MITRE ATT&CK framework for Industrial Control Systems. It explains that the ICS version is a community-sourced knowledge base mapping adversary tactics and behaviors specific to industrial environments, distinct from the IT-focused framework. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Nozomi Networks**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must name the source descriptor, the bounded claim about **Networks**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Nozomi Networks** work as a **cyber-physical tabletop evidence packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that Nozomi Networks: How Security Teams Use the ICS Framework establishes intent without reviewing alternative explanations.

Transfer task. Transfer **Nozomi Networks** to a second module by preserving safety-aware tabletop readiness and defensive coverage review, changing the source evidence, and naming a new reviewer.

64.2.3 MITRE ATT&CK for ICS worked safe example: synthetic inputs, evidence, and review

Worked example: a sample water-utility tabletop reviews synthetic process logs after a simulated anomaly. [255, 2026]; [257, 2026].

Triangulation anchors. In module 46's worked-example section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **safety-aware ICS and OT intelligence**. Learners use a **cyber-physical tabletop evidence packet** and keep this boundary visible: No live device control, unsafe process change, exploit sequence, evasion, or operational response.

Frame. The classroom question centers on **ICS Matrix: 12 Tactics, Full Technique Library**. Excluded actions stay explicit, and the **Cyber-Physical Readiness Lens** planning question is: Which asset, architecture record, consequence, operator decision, and recovery path is being exercised defensively?

Inputs. For the **ICS Matrix: 12 Tactics, Full Technique Library** scenario, use toy HMI screenshots, fabricated network alerts, public ICS control guidance, and a safety stop card. The Cyber-Physical Readiness Lens intake note records provenance, sensitivity, fit-to-purpose, and why the

fixture is enough for this bounded exercise.
Analysis. For **ICS Matrix: 12 Tactics, Full Technique Library**, students map assets to consequences, classify tabletop injects, identify human decisions, and preserve recovery evidence. Pause whenever an inference about ICS Matrix: 12 Tactics, Full Technique Library appears without evidence, confidence outruns support, or an agent output is treated as judgment.
Filled artifact. Purpose = **ICS Matrix: 12 Tactics, Full Technique Library** classroom scenario; unit artifact = cyber-physical tabletop evidence packet; evidence = allowed inputs; method = safety-aware tabletop readiness and defensive coverage review; output = a cyber-physical tabletop packet with assets, consequences, ATT&CK mapping, decisions, and debrief; boundary = no external action; reviewer = instructor or named peer.
Flawed answer to revise. Treating **ICS Matrix: 12 Tactics, Full Technique Library** as "Cyber-Physical Readiness Lens confirms it" is not enough. The revision ties the claim to safety-aware tabletop readiness and defensive coverage review, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.
Debrief. The reuse note for **ICS Matrix: 12 Tactics, Full Technique Library** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

64.2.4 MITRE ATT&CK for ICS practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Cyber-Physical Readiness Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**.
Triangulation anchors. In module 46's practice-sequence section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare ICS Matrix: 12 Tactics, Full Technique Library, Cyber access-and-execution taxonomy review using fabricated alerts, ICS controller-change coverage review using synthetic process records; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane.
2. Frame	Answer the lens question: Which asset, architecture record, consequence, operator decision, and recovery path is being exercised defensively?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for ICS Matrix: 12 Tactics, Full Technique Library: tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the cyber-physical tabletop evidence packet fields for ICS Matrix: 12 Tactics, Full Technique Library.	Unit profile note.	Evidence artifacts include asset-consequence map, operator decision log.
4. Challenge	Test the misconception that ICS Matrix: 12 Tactics, Full Technique Library is optional whenever separate cyber analysis from unsafe process control or live operational action feels inconvenient.	Failure-mode note.	The artifact applies the key distinction: separate cyber analysis from unsafe process control or live operational action.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

64.2.4.1 MITRE ATT&CK for ICS instructor notes: source reasoning, review points, and studio focus

Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**. [255, 2026]; [257, 2026].

64.2.4.2 MITRE ATT&CK for ICS extension exercise: peer validation and refresh trigger review

Evidence anchor. Section 64; [255, 2026].
Have learners swap artifacts and apply the **Cyber-Physical Readiness Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**.

64.2.5 MITRE ATT&CK for ICS knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 64; [255, 2026].

1. Explain how **ICS Matrix: 12 Tactics, Full Technique Library** is defined here; name the source descriptor that supports the definition.
2. Contrast **ICS Matrix: 12 Tactics, Full Technique Library** with **Cyber access-and-execution taxonomy review using fabricated alerts** using the **Cyber-Physical Readiness Lens** artifact fields.
3. Identify one failure mode from the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which cyber observation changes meaning once physical consequence is considered?
5. Correct this misconception: that ICS Matrix: 12 Tactics, Full Technique Library is optional whenever separate cyber analysis from unsafe process control or live operational action feels inconvenient.

64.2.5.1 MITRE ATT&CK for ICS answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **ICS Matrix: 12 Tactics, Full Technique Library** without source evidence, uncertainty, or a safe transfer task.

64.3 MITRE ATT&CK for ICS assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 64; [255, 2026].

64.3.1 MITRE ATT&CK for ICS evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 64; [255, 2026].

64.3.2 MITRE ATT&CK for ICS transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 64; [255, 2026].

64.3.2.1 MITRE ATT&CK for ICS lineage and source tradition: profile, concepts, and first anchors This sits in the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lineage: defensive intelligence for safety-critical environments where availability, engineering state, and physical consequence matter. [255, 2026]; [257, 2026].

64.3.2.2 MITRE ATT&CK for ICS working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 64; [255, 2026].
The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**, with provenance and reviewability throughout.

64.3.2.3 MITRE ATT&CK for ICS knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** synthetic process logs, asset/consequence maps, operator decisions, safety stops, and recovery evidence. [255, 2026]; [257, 2026].
- **Transforms:** asset-consequence mapping, ATT&CK-for-ICS coverage review, operator-decision rehearsal, and after-action learning.
- **Outputs:** cyber-physical tabletop packet, debrief rubric, recovery note, and control-coverage map.
- **Failure modes:** IT-first assumptions, unsafe actuation, live-control drift, and missing safety review.

64.3.2.4 MITRE ATT&CK for ICS transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 64; [255, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**.
- **Evidence contract:** keep the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as cyber-physical tabletop packet, debrief rubric, recovery note, and control-coverage map that another reviewer can audit.

64.3.2.5 MITRE ATT&CK for ICS profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 64; [255, 2026].
The matched profile emphasizes defensive intelligence for safety-critical environments where availability, engineering state, and physical consequence matter. The method stack is asset/consequence mapping, ATT&CK-for-ICS coverage review, defense-in-depth audit, remote-access check, and tabletop injects; the local topic cluster is **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**.

64.3.3 MITRE ATT&CK for ICS evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 64; [255, 2026].
Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** profile tells reviewers what evidence is strong enough for the module artifact built around **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**.

64.3.3.1 MITRE ATT&CK for ICS guide source spine: inherited keys and local citation roles Primary guide citations: [255, 2026]; [257, 2026]; [261, 2026]; [274, 2026]; [278, 2026]; [280, 2026]; [287, 2026]; [288, 2026]; [295, 2026]; [213, 2026]; [214, 2026]; [215, 2026]; [216, 2026].

64.3.3.2 MITRE ATT&CK for ICS verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [255, 2026]; [257, 2026].

Tier	What counts	How it is used
Source guide	[255, 2026]; [257, 2026]; [261, 2026]; [274, 2026]; [278, 2026]; [280, 2026]; [287, 2026]; [288, 2026]; [295, 2026]; [213, 2026]; [214, 2026]; [215, 2026]; [216, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 46's source-canon section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Maintenance rule: Perplexity may suggest candidates for **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts** and [255, 2026]; [257, 2026], but only directly verified source URLs are encoded as citations.

64.3.3.3 MITRE ATT&CK for ICS intelligence practice lens: evidence artifact and safety check Practice lens: **Cyber-Physical Readiness Lens** for **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**. [255, 2026]; [257, 2026].

Planning question: Which asset, architecture record, consequence, operator decision, and recovery path is being exercised defensively?

Evidence artifact: tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric.

Validation rule: validate against safety, availability, engineering state, incident scope, and after-action learning. Applied to **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**.

Handoff contract: separate cyber indicators, process observations, safety impact, operator choices, and recovery evidence.

Safety check: keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions.

64.3.3.4 MITRE ATT&CK for ICS runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 64; [255, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	46.99	46.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind MITRE ATT&CK for ICS to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Bounded autonomy, procurement, incident-response, and assurance studio	46.101	46.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for MITRE ATT&CK for ICS	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Model-card, recoverability, retention, and learner-support evidence package	46.102	46.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for MITRE ATT&CK for ICS	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
ICS Matrix: 12 Tactics, Full Technique Library	46.1	46.1 ICS Matrix: 12 Tactics, Full Technique Library	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Cyber access-and-execution taxonomy review using fabricated alerts	46.1.1	46.1.1 source title transformed into safe curriculum treatment; original: Initial Access (12 techniques): Drive-by, Remote Services, Wireless Compromise	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
ICS controller-change coverage review using synthetic process records	46.1.2	46.1.2 source title transformed into safe curriculum treatment; original: Execution: Modify Controller Tasking, Command-Line Interface	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
ICS firmware and project-integrity coverage	46.1.3	46.1.3 source title transformed into safe curriculum treatment; original: Persistence: Modify Firmware (System and Module), Project File Infection	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
ICS evasion coverage-control review using defensive detection questions	46.1.4	46.1.4 source title transformed into safe curriculum treatment; original: Evasion: Rootkit, Masquerading, Indicator Removal	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
ICS defensive coverage and safety tabletop using synthetic process records	46.1.5	46.1.5 source title transformed into safe curriculum treatment; original: Discovery: Remote System Discovery, Network Sniffing	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Cyber credential-and-movement taxonomy review using fabricated alerts	46.1.6	46.1.6 source title transformed into safe curriculum treatment; original: Lateral Movement: Lateral Tool Transfer, Valid Accounts	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
ICS collection-risk detection review using synthetic tag records	46.1.7	46.1.7 source title transformed into safe curriculum treatment; original: Collection: I/O Image, Monitor Process State, Point & Tag Identification	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
ICS alarm and communications-resilience tabletop	46.1.8	46.1.8 source title transformed into safe curriculum treatment; original: Inhibit Response Function: Alarm Suppression, Block Communications	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
ICS process-safety consequence review using synthetic records	46.1.9	46.1.9 source title transformed into safe curriculum treatment; original: Impair Process Control: Brute Force I/O, Modify Parameter	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
ICS defensive coverage and safety tabletop using synthetic process records	46.1.10	46.1.10 source title transformed into safe curriculum treatment; original: Impact: Damage to Property, Loss of Safety, Manipulation of Control	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Using ICS ATT&CK in Risk Assessment (ISA InTech)	46.2	46.2 Using ICS ATT&CK in Risk Assessment (ISA InTech)	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Dragos: MITRE ATT&CK for ICS Threat Actor Mapping	46.3	46.3 Dragos: MITRE ATT&CK for ICS Threat Actor Mapping	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Nozomi Networks: How Security Teams Use the ICS Framework	46.4	46.4 Nozomi Networks: How Security Teams Use the ICS Framework	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions

64.3.3.5 MITRE ATT&CK for ICS reusable subsection contract: topic rows, artifacts, and safety duties **Evidence anchor.** Section 64; [255, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
ICS Matrix: 12 Tactics, Full Technique Library	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Cyber access-and-execution taxonomy review using fabricated alerts	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
ICS controller-change coverage review using synthetic process records	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
ICS firmware and project-integrity coverage	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
ICS evasion coverage-control review using defensive detection questions	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
ICS defensive coverage and safety tabletop using synthetic process records	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Cyber credential-and-movement taxonomy review using fabricated alerts	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
ICS collection-risk detection review using synthetic tag records	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
ICS alarm and communications-resilience tabletop	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
ICS process-safety consequence review using synthetic records	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Impact: ICS defensive coverage and safety tabletop using synthetic process records	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Using ICS ATT&CK in Risk Assessment (ISA InTech)	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Dragos: MITRE ATT&CK for ICS Threat Actor Mapping	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Nozomi Networks: How Security Teams Use the ICS Framework	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions

64.3.3.6 MITRE ATT&CK for ICS annotated source ledger: real titles and local contribution Each source cited by this **ICS/OT Cyber-Physical Defense and Tabletop Readiness** module is paired below with its real title and a one-line note on what it contributes to **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**.

Source	Cited work	What it contributes	Status
[255, 2026]	Web of Things (WoT) Architecture 1.1	The W3C Recommendation for Web of Things Architecture 1.1, published in December 2023, defining an abstract architecture for interoperability across diverse Internet of Things platforms. It introduces core concepts including Things described by machine-readable Thing Descriptions, reusable Thing Models, and Consumers that interpret descriptions to interact via Properties, Actions, and Events.	verified source-guide
[257, 2026]	Web of Things (WoT) Discovery	A W3C Recommendation for Web of Things (WoT) Discovery, published December 5, 2023 by the W3C Web of Things Working Group. It specifies how IoT devices and services can be discovered and how their Thing Description metadata can be accessed securely, using a two-phase model of Introduction and Exploration.	verified source-guide
[261, 2026]	RFC 9110: HTTP Semantics	RFC 9110, the official IETF standards document defining the core semantics and architecture of HTTP, published in June 2022 and consolidating nine earlier RFCs. It establishes terminology and protocol aspects shared across HTTP versions, including methods, status codes, header fields, content negotiation, conditional and range requests, authentication, and the http and https URI schemes.	verified source-guide
[274, 2026]	CAST Universal Design for Learning Guidelines version 3.0	The official CAST website for the Universal Design for Learning (UDL) Guidelines version 3.0, released in 2024. The framework offers research-based guidance for designing inclusive learning environments and is organized around three principles: Engagement (motivation and emotional support), Representation (accessible presentation of information), and Action and Expression (diverse means of participation and communication).	verified source-guide
[278, 2026]	Recommendation of the Council on Public Procurement	The OECD Recommendation of the Council on Public Procurement (OECD/LEGAL/0411), a legal instrument adopted by the OECD Council in 2015 on the proposal of the Public Governance Committee. It frames public procurement as a pillar of strategic governance and service delivery and sets out principles for governments to follow.	verified source-guide
[280, 2026]	NIST SP 800-61 Rev. 3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management	NIST SP 800-61 Rev. 3, published April 2025, integrates incident response guidance into broader cybersecurity risk management aligned with the NIST Cybersecurity Framework 2.0, superseding the 2012 Rev. 2. The publication addresses cyber threat information sharing, incident handling and management practices, and procedures for detecting, responding to, and recovering from security incidents.	verified source-guide

Source	Cited work	What it contributes	Status
[287, 2026]	Datasheets for Datasets	A 2018 arXiv paper proposing 'datasheets for datasets,' a standardized documentation framework for machine learning datasets modeled on electronic component datasheets. The authors argue the field lacks consistent dataset documentation, which creates risk in high-stakes applications, and propose that datasets be accompanied by documentation covering motivation, composition, collection process, recommended uses, and test results.	verified source-guide
[288, 2026]	Algorithmic Transparency Recording Standard Hub	A GOV.UK collection page serving as the hub for the UK Algorithmic Transparency Recording Standard (ATRS), maintained by the Government Digital Service. It provides a standardized template for documenting public-sector use of algorithmic tools, completion guidance, policy on scope and compliance, and a searchable repository of published transparency records.	verified source-guide
[295, 2026]	M-25-22: Driving Efficient Acquisition of Artificial Intelligence in Government	OMB Memorandum M-25-22 (April 3, 2025), Driving Efficient Acquisition of Artificial Intelligence in Government, issued under Executive Order 13960 and related directives. It provides guidance to federal agencies for acquiring effective and trustworthy AI in a timely, cost-effective manner, and rescinds and replaces earlier memorandum M-24-18.	verified source-guide
[213, 2026]	ICS Matrix - MITRE ATT&CK®	The Industrial Control Systems (ICS) domain of the MITRE ATT&CK framework, a knowledge base documenting adversary behaviors based on real-world observations of attacks on critical infrastructure. The matrix organizes methods into twelve tactical categories spanning initial access through impact, including ICS-specific concerns such as firmware modification and disruption of operational technology.	verified source-guide
[214, 2026]	Cybersecurity Using ICS ATT&CK Strategies	A June 2021 InTech Magazine article by Jacob Chapman, published by the International Society of Automation, on using the ICS ATT&CK framework to strengthen cybersecurity for manufacturing and industrial IoT systems. It describes a three-phase risk-management approach: gathering information on assets and network architecture, mapping potential attack paths to identify vulnerabilities, and prioritizing mitigations by impact.	verified source-guide

Source	Cited work	What it contributes	Status
[215, 2026]	MITRE ATT&CK for ICS Framework - Dragos	A Dragos solutions page describing the MITRE ATT&CK for ICS framework, a knowledge base of adversary behaviors observed in attacks against industrial control system networks. It explains how the Dragos Platform maps detections to ATT&CK tactics and techniques through regular knowledge updates, profiles named threat groups, and organizes behaviors across tactic areas spanning initial access through impact scenarios such as loss of control, safety, or availability.	verified source-guide
[216, 2026]	How to Use the MITRE ATT&CK Framework for ICS - Nozomi Networks	A Nozomi Networks resource (a 2020 webinar) on how security teams apply the MITRE ATT&CK framework for Industrial Control Systems. It explains that the ICS version is a community-sourced knowledge base mapping adversary tactics and behaviors specific to industrial environments, distinct from the IT-focused framework.	verified source-guide

Where this sits. This module's overview is Section 64; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

64.3.4 MITRE ATT&CK for ICS governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 64; [255, 2026].

64.3.5 MITRE ATT&CK for ICS analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 46's governance-boundary section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **ICS/OT Cyber-Physical Defense and Tabletop Readiness** for **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**. [255, 2026]; [257, 2026].

Curriculum topic spine: ICS Matrix: 12 Tactics, Full Technique Library, **Cyber access-and-execution taxonomy review using fabricated alerts**, **ICS controller-change coverage review using synthetic process records**. **Verified anchor cluster:** [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]; [Cybersecurity and Agency, 2026a]; [Cybersecurity and Agency, 2026c]; [MITRE, 2026c].

Conceptual depth: defensive intelligence for safety-critical environments where availability, engineering state, and physical consequence matter.

Method stack: asset/consequence mapping, ATT&CK-for-ICS coverage review, defense-in-depth audit, remote-access check, and tabletop injects.

Composability contract: separate cyber indicators, engineering observations, safety impacts, operator decisions, and recovery actions.

Known failure modes: IT-first assumptions, unsafe automation, untested shutdown logic, poor remote-access control, and missing after-action learning.

Defensive boundary: all ICS work remains tabletop, lab, or accountable defensive review; no exploitation, unsafe process manipulation, or live control actions. Applied to **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**.

Anchor	Why it matters here
[of Standards and Technology, 2024f]	Official cybersecurity-risk governance framework that adds the Govern function and supplies a common language for AI, OT, and enterprise risk. Checked as of 2026-05-21; role: curriculum_anchor.
[of Standards and Technology, 2022b]	Systems-security engineering foundation for trustworthy systems in contested operational environments and related training programs. Checked as of 2026-05-21; role: curriculum_anchor.
[of Standards and Technology, 2024b]	Official NIST operational technology security guidance. Checked as of 2026-05-21; role: source_quality_anchor.
[of Automation, 2026]	Official ISA overview of industrial automation and control security standards. Checked as of 2026-05-21; role: source_quality_anchor.
[Cybersecurity and Agency, 2026a]	Official prioritized baseline of IT and OT cybersecurity practices for critical-infrastructure risk reduction and maturity assessment. Checked as of 2026-05-21; role: curriculum_anchor.
[Cybersecurity and Agency, 2026c]	Official defensive ICS practice library for defense-in-depth, forensics, incident response, and remote access. Checked as of 2026-05-21; role: curriculum_anchor.
[MITRE, 2026c]	Threat-informed defensive matrix for ICS tactics and techniques, used for coverage mapping. Checked as of 2026-05-21; role: curriculum_anchor.

64.3.5.1 MITRE ATT&CK for ICS evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [255, 2026]; [257, 2026].

64.3.6 MITRE ATT&CK for ICS agentic boundary: assist, approve, block, and record

Evidence anchor. Section 64; [255, 2026].

AGEINT translation is bounded by the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**.

64.3.6.1 MITRE ATT&CK for ICS permitted defensive utility: curriculum uses and safe outputs

Evidence anchor. Section 64; [255, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**.

64.3.6.2 MITRE ATT&CK for ICS excluded operational boundary: blocked actions and stop rules

Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [255, 2026]; [257, 2026] and **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

64.3.7 MITRE ATT&CK for ICS governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 64; [255, 2026].

Governance is practiced as a gate on the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane. Learners use the **Cyber-Physical Readiness Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**.

64.3.7.1 MITRE ATT&CK for ICS governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [255, 2026]; [257, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **ICS/OT Cyber-Physical Defense and Tabletop Readiness** failure modes and the **Cyber-Physical Readiness Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

64.3.7.2 MITRE ATT&CK for ICS evidence package handoff: appendices, records, and reuse Evidence anchor. Section 64; [255, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Cyber-Physical Readiness Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**.

64.3.7.3 MITRE ATT&CK for ICS current-source assurance: verified anchors and local artifact fit The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**. [255, 2026]; [257, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_nist_csf_2` for **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**?	The NIST Cybersecurity Framework (CSF) 2.0; lane `ics_ot_defense`; checked 2026-05-21.	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric; Official cybersecurity-risk governance framework that adds the Govern function and supplies a common language for AI, OT, and enterprise risk.
What does the module inherit from `official_nist_sp_800_160r1` for **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**?	Engineering Trustworthy Secure Systems, NIST SP 800-160 Vol. 1 Rev. 1; lane `ics_ot_defense`; checked 2026-05-21.	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric; Systems-security engineering foundation for trustworthy systems in contested operational environments and related training programs.
What does the module inherit from `official_nist_sp_800_82r3` for **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**?	Guide to Operational Technology Security, NIST SP 800-82 Rev. 3; lane `source_quality_spine`; checked 2026-05-21.	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric; Official NIST operational technology security guidance.
What does the module inherit from `official_isa_iec_62443` for **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**?	ISA/IEC 62443 Series of Standards; lane `source_quality_spine`; checked 2026-05-21.	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric; Official ISA overview of industrial automation and control security standards.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 64; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

64.3.8 MITRE ATT&CK for ICS assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 64; [255, 2026].

64.3.9 MITRE ATT&CK for ICS assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 64; [255, 2026].

64.3.9.1 MITRE ATT&CK for ICS capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts** and [255, 2026]; [257, 2026].

64.3.9.2 MITRE ATT&CK for ICS instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts** and [255, 2026]; [257, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

64.3.9.3 MITRE ATT&CK for ICS assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
ICS Matrix: 12 Tactics, Full Technique Library	Completed **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Cyber access-and-execution taxonomy review using fabricated alerts	Completed **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
ICS controller-change coverage review using synthetic process records	Completed **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

64.3.10 MITRE ATT&CK for ICS refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [255, 2026]; [257, 2026] and **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**.

64.3.10.1 MITRE ATT&CK for ICS refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**. The local signals begin with [255, 2026]; [257, 2026].

64.3.10.2 MITRE ATT&CK for ICS claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**, and the source spine for these checks begins with [255, 2026]; [257, 2026].

64.3.11 MITRE ATT&CK for ICS reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [255, 2026]; [257, 2026].

Triangulation anchors. In module 46's review-checklist section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts**. [255, 2026]; [257, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

64.3.12 MITRE ATT&CK for ICS learning-path links: module map, overview, and curriculum atlas

Use the cross-links below to place **ICS Matrix: 12 Tactics, Full Technique Library; Cyber access-and-execution taxonomy review using fabricated alerts** in the wider unit: the orientation sets the frame, the parent unit supplies the shared safety posture, and the neighbouring modules show what evidence enters and leaves. Lead sources: [255, 2026]; [257, 2026].

Section 2, Section 62, Section 63, Section 65

65 Historical ICS Cyber Incidents: Intelligence Analysis

65.0.1 Historical ICS Cyber Incidents: Intelligence Analysis figures and course links: visual evidence, source flow, and navigation

The module uses Figure 139 and Figure 134 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.

Navigation links: Section 2, Section 62, Section 64, Section 66.

This module teaches the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane through a bounded, source-backed coursebook chapter. [252, 2026]; [255, 2026].

65.1 ICS/OT Cyber-Physical Defense and Tabletop Readiness frame for Historical ICS Cyber Incidents: Intelligence Analysis: source context, topic focus, and reader task

Evidence anchor. Section 65; [252, 2026].

65.1.1 Historical ICS Cyber Incidents: Intelligence Analysis orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 65; [252, 2026].

65.1.2 Historical ICS Cyber Incidents: Intelligence Analysis conceptual primer: source context, core model, and reader task

This chapter teaches ICS/OT intelligence as safety-aware defensive reasoning: asset state, engineering consequence, operator decision, and recovery evidence matter as much as cyber indicators. The chapter uses **Cyber-Physical Readiness Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**.

The central distinction is to separate cyber analysis from unsafe process control or live operational action. Core topics include **Evaluation Framework for ICS Cyber Incidents (ScienceDirect 2021); The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex; Stuxnet: First Cyber-Physical Weapon — Operation Olympic Games**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.

Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [252, 2026]; [255, 2026].

Learners move from vocabulary and the **Cyber-Physical Readiness Lens** distinction through topic lessons on **Evaluation Framework for ICS Cyber Incidents (ScienceDirect 2021)** with evidence and misconception checks, then assemble a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** with safety and rights gates.

65.1.3 Historical ICS Cyber Incidents: Intelligence Analysis learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 65; [252, 2026].

- Connect **Evaluation Framework for ICS Cyber Incidents (ScienceDirect 2021) and The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex** to **ICS/OT Cyber-Physical Defense and Tabletop Readiness** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate cyber analysis from unsafe process control or live operational action; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as IT-first assumptions, unsafe automation, untested shutdown logic, poor remote-access control, and missing after-action learning, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: all ICS work remains tabletop, lab, or accountable defensive review; no exploitation, unsafe process manipulation, or live control actions.

65.1.4 Historical ICS Cyber Incidents: Intelligence Analysis core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 65; [252, 2026].

Term	Working definition
Engineering state	the physical or process condition that gives cyber evidence safety meaning
Consequence	the operational, safety, environmental, or service effect of a condition
Defense in depth	layered prevention, detection, response, and recovery controls
Tabletop inject	a synthetic event used to rehearse decisions without touching live systems
Recovery evidence	proof that a safe state, service, or learning objective was restored
Evaluation Framework for ICS Cyber Incidents…	Key terms: Evaluation, Framework, ICS.
The Cyber-Physical Six: Stuxnet, BlackEnergy,…	Key terms: Cyber, Physical, Six.

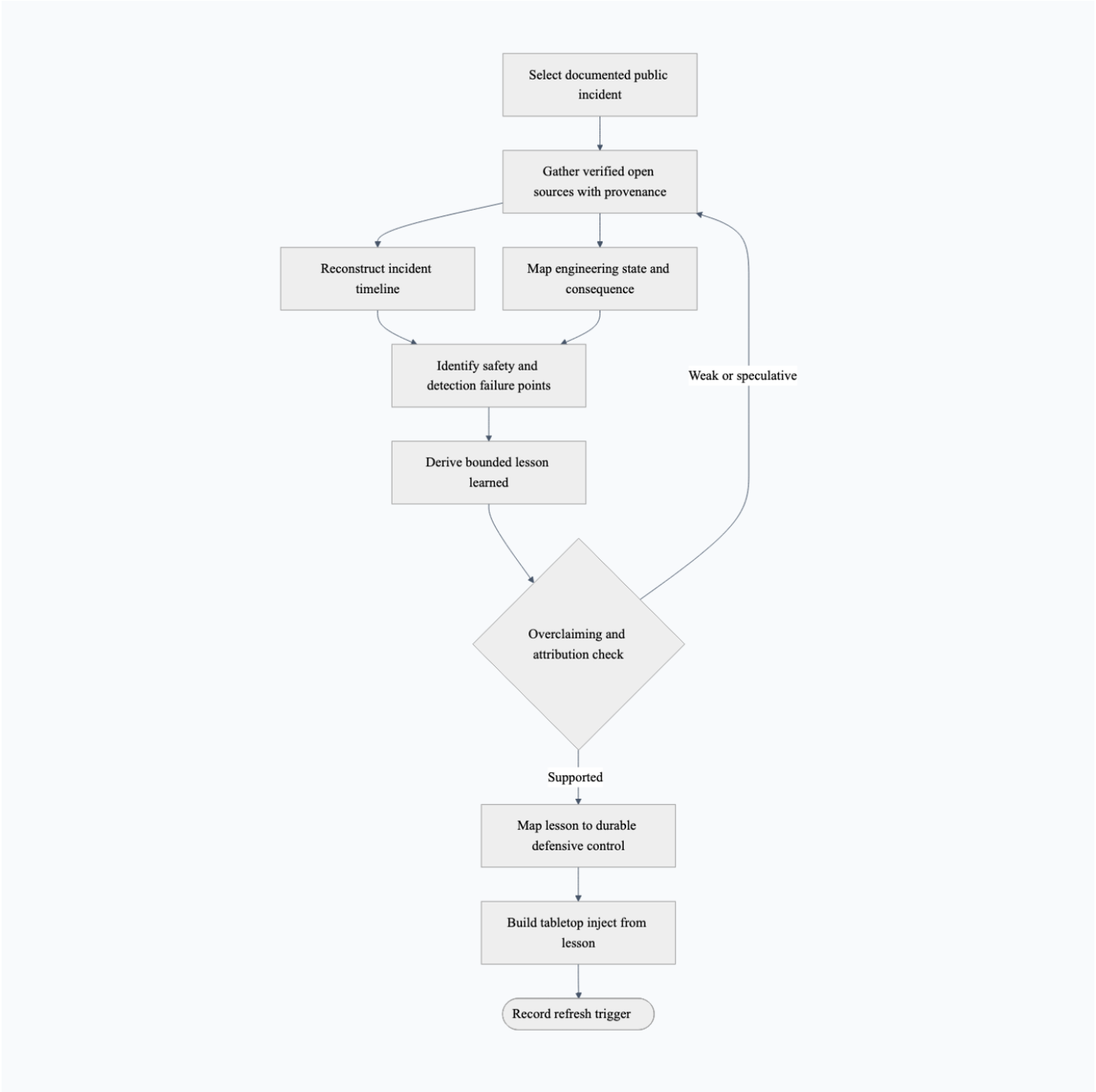


Figure 139: A learning framework that turns a studied historical incident into reconstructed timeline, engineering consequence, lesson, and durable defensive control. In the industrial and cyber physical intelligence / historical ics cyber incidents intelligence analysis section, it lets readers compare Select documented public incident, Gather verified open sources with provenance, Reconstruct incident timeline, and Map engineering state and consequence so the visual functions as a traceable course aid rather than an unscoped assertion.

65.2 Cyber-Physical Readiness Lens path for Historical ICS Cyber Incidents: Intelligence Analysis: lesson cluster, safe artifact, and review

Evidence anchor. Section 65; [252, 2026].

65.2.1 Historical ICS Cyber Incidents: Intelligence Analysis practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 65; [252, 2026].

65.2.2 Historical ICS Cyber Incidents: Intelligence Analysis topic lessons: source-backed concepts and transfer tasks

This module builds ICS/OT intelligence as safety-aware defensive reasoning: asset state, engineering consequence, operator decision, and recovery evidence matter as much as cyber indicators. The sequence opens with **Evaluation Framework for ICS Cyber Incidents (ScienceDirect 2021)**, **The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**, **Stuxnet: First Cyber-Physical Weapon — Operation Olympic Games** and applies the **Cyber-Physical Readiness Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 134; module overview Section 65; curriculum atlas Section 2.

Triangulation anchors. In module 47's topic-lessons section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

65.2.2.1 Lesson 1: Evaluation Framework for ICS Cyber Incidents (ScienceDirect 2021) Concept. Evaluation Framework for ICS Cyber Incidents (ScienceDirect 2021) applies Evaluation, Framework, ICS within ICS/OT Cyber-Physical Defense and Tabletop Readiness: learners use separate cyber analysis from unsafe process control or live operational action and safety-aware tabletop readiness and defensive coverage review evidence before any judgment moves forward.

Why it matters. Evaluation Framework matters in the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane because safety-aware tabletop readiness and defensive coverage evidence must stay separate from judgment; IT-first assumptions is a common failure.

Source support. Evaluation Framework for ICS Cyber Incidents (ScienceDirect 2021) rests on [217, 2026]. Its anchor reference records: We analyze six significant ICS cyber incidents in the energy and power industries, namely Stuxnet. Use it for the claim that **Evaluation Framework for ICS Cyber Incidents (ScienceDirect 2021)** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. Ground **Evaluation Framework** in the evidence the row cites. [217, 2026] We analyze six significant ICS cyber incidents in the energy and power industries, namely Stuxnet. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Evaluation Framework**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must name the source descriptor, the bounded claim about **Evaluation Framework for ICS Cyber**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Evaluation Framework** work as a **cyber-physical tabletop evidence packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that Evaluation Framework for ICS Cyber Incidents (ScienceDirect 2021) is optional whenever separate cyber analysis from unsafe process control or live operational action feels inconvenient.

Transfer task. Transfer **Evaluation Framework** to a second module by preserving safety-aware tabletop readiness and defensive coverage review, changing the source evidence, and naming a new reviewer.

65.2.2.2 Lesson 2: The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex Concept. The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex studies the incident as a tabletop lesson in safety consequence, attribution caution, and defensive coverage—not as attack replication.

Why it matters. Analysts use **The Cyber-Physical Six** to separate cyber analysis from unsafe process control or live operational action. A defensible treatment names the judgment it enables for safety-aware tabletop readiness and defensive coverage review, the proof limit that IT-first assumptions would otherwise hide, and the reviewer accountable for challenge.

Source support. The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex rests on [218, 2026]. Its anchor reference records: An executive research report from Honeywell's Global Analysis, Research, and Defense group titled "The Cyber-Physical Six," tracing how targeted industrial attacks have evolved and predicting future trends. Use it for pinning down the scope of **The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. Read **The Cyber-Physical Six** against the works cited for this row. [218, 2026] An executive research report from Honeywell's Global Analysis, Research, and Defense group titled "The Cyber-Physical Six," tracing how targeted industrial attacks have evolved and predicting future trends. It reviews six landmark cyber-physical attacks affecting industrial control and operational technology systems, then analyzes observed trends such as modularity, expanding capabilities, and the increasing frequency of new attack tools. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **The Cyber-Physical Six**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must name the source descriptor, the bounded claim about **Cyber-Physical Six**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **The Cyber-Physical Six** work as a **cyber-physical tabletop evidence packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex establishes intent without reviewing alternative explanations.

Transfer task. Transfer **The Cyber-Physical Six** to a second module by preserving safety-aware tabletop readiness and defensive coverage review, changing the source evidence, and naming a new reviewer.

65.2.2.3 Lesson 3: Stuxnet: First Cyber-Physical Weapon — Operation Olympic Games Concept. Stuxnet: First Cyber-Physical Weapon — Operation Olympic Games studies the incident as a tabletop lesson in safety consequence, attribution caution, and defensive coverage—not as attack replication.

Why it matters. Without explicit treatment of **Stuxnet: First Cyber-Physical Weapon — Operation Olympic Games**, IT-first assumptions undermines safety-aware tabletop readiness and defensive coverage review; the lesson builds the habit to separate cyber analysis from unsafe process control or live operational action.

Source support. Stuxnet: First Cyber-Physical Weapon — Operation Olympic Games rests on [219, 2026] and [220, 2026]. The lead source's own note reads: Journalist Kim Zetter testified before Congress on how Stuxnet demonstrated that physical infrastructure could be destroyed through malicious code alone, targeting Siemens programmable logic controllers at Iran's Natanz uranium enrichment facility. Use them for pinning down the scope of **Stuxnet: First Cyber-Physical Weapon — Operation Olympic Games**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. Ground **Stuxnet: First Cyber-Physical Weapon — Operation Olympic Games** in the evidence the row cites. [219, 2026] I've been asked specifically to describe how. [220, 2026] Journalist Kim Zetter testified before Congress on how Stuxnet demonstrated that physical infrastructure could be destroyed through malicious code alone, targeting Siemens programmable logic controllers at Iran's Natanz uranium enrichment facility. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Stuxnet**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must name the source descriptor, the bounded claim about **Stuxnet**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Stuxnet: First Cyber-Physical Weapon — Operation Olympic Games** work as a **cyber-physical tabletop evidence packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that Stuxnet: First Cyber-Physical Weapon — Operation Olympic Games replaces human review whenever evidence looks plausible.

Transfer task. Transfer **Stuxnet: First Cyber-Physical Weapon — Operation Olympic Games** to a second module by preserving safety-aware tabletop readiness and defensive coverage review, changing the source evidence, and naming a new reviewer.

65.2.2.4 Lesson 4: BlackEnergy: Ukraine Power Grid Attacks (2015)

Concept. BlackEnergy: Ukraine Power Grid Attacks (2015) reads the outage case through engineering state, operator decisions, and recovery evidence in a synthetic tabletop.

Why it matters. Analysts use **BlackEnergy: Ukraine Power Grid Attacks (2015)** to separate cyber analysis from unsafe process control or live operational action. A defensible treatment names the judgment it enables for safety-aware tabletop readiness and defensive coverage review, the proof limit that IT-first assumptions would otherwise hide, and the reviewer accountable for challenge.

Source support. BlackEnergy: Ukraine Power Grid Attacks (2015) rests on [218, 2026]. Its anchor reference records: An executive research report from Honeywell's Global Analysis, Research, and Defense group titled "The Cyber-Physical Six," tracing how targeted industrial attacks have evolved and predicting future trends. Use it for pinning down the scope of **BlackEnergy: Ukraine Power Grid Attacks (2015)**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. Ground **BlackEnergy: Ukraine Power Grid Attacks (2015)** in the evidence the row cites. [218, 2026] An executive research report from Honeywell's Global Analysis, Research, and Defense group titled "The Cyber-Physical Six," tracing how targeted industrial attacks have evolved and predicting future trends. It reviews six landmark cyber-physical attacks affecting industrial control and operational technology systems, then analyzes observed trends such as modularity, expanding capabilities, and the increasing frequency of new attack tools. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **BlackEnergy**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must name the source descriptor, the bounded claim about **BlackEnergy**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **BlackEnergy: Ukraine Power Grid Attacks (2015)** work as a **cyber-physical tabletop evidence packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that BlackEnergy: Ukraine Power Grid Attacks (2015) can be used while ignoring the rule to separate cyber analysis from unsafe process control or live operational action.

Transfer task. Transfer **BlackEnergy: Ukraine Power Grid Attacks (2015)** to a second module by preserving safety-aware tabletop readiness and defensive coverage review, changing the source evidence, and naming a new reviewer.

65.2.2.5 Lesson 5: CrashOverride/Industroyer: Protocol-Agnostic Power Grid Weapon

Concept. CrashOverride/Industroyer: Protocol-Agnostic Power Grid Weapon maps protocol-aware disruption to defensive detection questions and recovery evidence in synthetic records.

Why it matters. Without explicit treatment of **CrashOverride/Industroyer**, IT-first assumptions undermines safety-aware tabletop readiness and defensive coverage review; the lesson builds the habit to separate cyber analysis from unsafe process control or live operational action.

Source support. CrashOverride/Industroyer: Protocol-Agnostic Power Grid Weapon rests on [217, 2026]. The lead source's own note reads: We analyze six significant ICS cyber incidents in the energy and power industries, namely Stuxnet. Use it for fixing what **CrashOverride/Industroyer: Protocol-Agnostic Power Grid Weapon** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. Ground **CrashOverride/Industroyer** in the evidence the row cites. [217, 2026] We analyze six significant ICS cyber incidents in the energy and power industries, namely Stuxnet. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **CrashOverride/Industroyer**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must name the source descriptor, the bounded claim about **CrashOverride/Industroyer**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **CrashOverride/Industroyer** work as a **cyber-physical tabletop evidence packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that CrashOverride/Industroyer: Protocol-Agnostic Power Grid Weapon is optional whenever separate cyber analysis from unsafe process control or live operational action feels inconvenient.

Transfer task. Transfer **CrashOverride/Industroyer** to a second module by preserving safety-aware tabletop readiness and defensive coverage review, changing the source evidence, and naming a new reviewer.

65.2.2.6 Lesson 6: Triton/Trisis: Safety Instrumented System Attack

Concept. Triton/Trisis: Safety Instrumented System Attack focuses on safety-system integrity, operator escalation, and consequence mapping—not live process manipulation.

Why it matters. Analysts use **Triton/Trisis** to separate cyber analysis from unsafe process control or live operational action. A defensible treatment names the judgment it enables for safety-aware tabletop readiness and defensive coverage review, the proof limit that IT-first assumptions would otherwise hide, and the reviewer accountable for challenge.

Source support. Triton/Trisis: Safety Instrumented System Attack rests on [217, 2026]. The lead source's own note reads: We analyze six significant ICS cyber incidents in the energy and power industries, namely Stuxnet. Use it for the claim that **Triton/Trisis: Safety Instrumented System Attack** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. Read **Triton/Trisis** against the works cited for this row. [217, 2026] We analyze six significant ICS cyber incidents in the energy and power industries, namely Stuxnet. Read each cited work for what it can support about this topic, where that claim originated, how

confident it is, and what evidence would change it.

Student artifact. For **Triton/Trisis**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must name the source descriptor, the bounded claim about **Triton/Trisis**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Triton/Trisis** work as a **cyber-physical tabletop evidence packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that Triton/Trisis: Safety Instrumented System Attack establishes intent without reviewing alternative explanations.

Transfer task. Transfer **Triton/Trisis** to a second module by preserving safety-aware tabletop readiness and defensive coverage review, changing the source evidence, and naming a new reviewer.

65.2.2.7 Lesson 7: Irongate: Stuxnet Descendant Against Simulated Environment Concept. Irongate: Stuxnet Descendant Against Simulated Environment studies the incident as a tabletop lesson in safety consequence, attribution caution, and defensive coverage—not as attack replication.

Why it matters. Without explicit treatment of **Irongate: Stuxnet Descendant Against Simulated Environment**, IT-first assumptions undermines safety-aware tabletop readiness and defensive coverage review; the lesson builds the habit to separate cyber analysis from unsafe process control or live operational action.

Source support. Irongate: Stuxnet Descendant Against Simulated Environment rests on [217, 2026]. The lead source's own note reads: We analyze six significant ICS cyber incidents in the energy and power industries, namely Stuxnet. Use it for fixing what **Irongate: Stuxnet Descendant Against Simulated Environment** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. Read **Irongate: Stuxnet Descendant Against Simulated Environment** against the works cited for this row. [217, 2026] We analyze six significant ICS cyber incidents in the energy and power industries, namely Stuxnet. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Irongate**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must name the source descriptor, the bounded claim about **Irongate**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Irongate: Stuxnet Descendant Against Simulated Environment** work as a **cyber-physical tabletop evidence packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that Irongate: Stuxnet Descendant Against Simulated Environment replaces human review whenever evidence looks plausible.

Transfer task. Transfer **Irongate: Stuxnet Descendant Against Simulated Environment** to a second module by preserving safety-aware tabletop readiness and defensive coverage review, changing the source evidence, and naming a new reviewer.

65.2.2.8 Lesson 8: Havex: IT-OT Pivot Using Weaponized OPC Software Concept. Havex: IT-OT Pivot Using Weaponized OPC Software uses supply-chain and HMI-trust motifs to review provenance, segmentation, and tabletop detection gaps.

Why it matters. Havex: IT-OT Pivot Using Weaponized OPC Software connects classroom vocabulary to ICS/OT Cyber-Physical Defense and Tabletop Readiness practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Havex: IT-OT Pivot Using Weaponized OPC Software rests on [217, 2026]. The most specific cited work observes: We analyze six significant ICS cyber incidents in the energy and power industries, namely Stuxnet. Use it for the claim that **Havex: IT-OT Pivot Using Weaponized OPC Software** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. Read **Havex: IT-OT Pivot Using Weaponized OPC Software** against the works cited for this row. [217, 2026] We analyze six significant ICS cyber incidents in the energy and power industries, namely Stuxnet. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Havex**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must name the source descriptor, the bounded claim about **Havex**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Havex: IT-OT Pivot Using Weaponized OPC Software** work as a **cyber-physical tabletop evidence packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that Havex: IT-OT Pivot Using Weaponized OPC Software can be used while ignoring the rule to separate cyber analysis from unsafe process control or live operational action.

Transfer task. Transfer **Havex: IT-OT Pivot Using Weaponized OPC Software** to a second module by preserving safety-aware tabletop readiness and defensive coverage review, changing the source evidence, and naming a new reviewer.

65.2.2.9 Lesson 9: Threat Scoring Framework: Malware Sophistication × Attack Consequence Concept. Threat Scoring Framework: Malware Sophistication × Attack Consequence applies Threat, Scoring, Framework within ICS/OT Cyber-Physical Defense and Tabletop Readiness: learners use separate cyber analysis from unsafe process control or live operational action and safety-aware tabletop readiness and defensive coverage review evidence before any judgment moves forward.

Why it matters. Without explicit treatment of **Threat Scoring Framework**, IT-first assumptions undermines safety-aware tabletop readiness and defensive coverage review; the lesson builds the habit to separate cyber analysis from unsafe process control or live operational action.

Source support. Threat Scoring Framework: Malware Sophistication × Attack Consequence rests on [217, 2026]. The most specific cited work observes: We analyze six significant ICS cyber incidents in the energy and power industries, namely Stuxnet. Use it for pinning down the scope of **Threat Scoring Framework: Malware Sophistication × Attack Consequence**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. Ground **Threat Scoring Framework** in the evidence the row cites. [217, 2026] We analyze six significant ICS cyber incidents in the energy and power industries, namely Stuxnet. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Threat Scoring Framework**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must name the source descriptor, the bounded claim about **Threat Scoring Framework**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Threat Scoring Framework** work as a **cyber-physical tabletop evidence packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that Threat Scoring Framework: Malware Sophistication × Attack Consequence is optional whenever separate cyber analysis from unsafe process control or live operational action feels inconvenient.

Transfer task. Transfer **Threat Scoring Framework** to a second module by preserving safety-aware tabletop readiness and defensive coverage review, changing the source evidence, and naming a new reviewer.

65.2.3 Historical ICS Cyber Incidents: Intelligence Analysis worked safe example: synthetic inputs, evidence, and review

Worked example: a sample water-utility tabletop reviews synthetic process logs after a simulated anomaly. [252, 2026]; [255, 2026].

Triangulation anchors. In module 47's worked-example section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **safety-aware ICS and OT intelligence**. Learners use a **cyber-physical tabletop evidence packet** and keep this boundary visible: No live device control, unsafe process change, exploit sequence, evasion, or operational response.

Frame. The classroom question centers on **Evaluation Framework for ICS Cyber Incidents (ScienceDirect 2021)**. Excluded actions stay explicit, and the **Cyber-Physical Readiness Lens** planning question is: Which asset, architecture record, consequence, operator decision, and recovery path is being exercised defensively?

Inputs. For the **Evaluation Framework for ICS Cyber Incidents** scenario, use toy HMI screenshots, fabricated network alerts, public ICS control guidance, and a safety stop card. The Cyber-Physical Readiness Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Evaluation Framework for ICS Cyber Incidents**, students map assets to consequences, classify tabletop injects, identify human decisions, and preserve recovery evidence. Pause whenever an inference about Evaluation Framework for ICS Cyber Incidents appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Evaluation Framework for ICS Cyber Incidents** classroom scenario; unit artifact = cyber-physical tabletop evidence packet; evidence = allowed inputs; method = safety-aware tabletop readiness and defensive coverage review; output = a cyber-physical tabletop packet with assets, consequences, ATT&CK mapping, decisions, and debrief; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Evaluation Framework for ICS Cyber Incidents** as "Cyber-Physical Readiness Lens confirms it" is not enough. The revision ties the claim to safety-aware tabletop readiness and defensive coverage review, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Evaluation Framework for ICS Cyber Incidents** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

65.2.4 Historical ICS Cyber Incidents: Intelligence Analysis practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Cyber-Physical Readiness Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**.

Triangulation anchors. In module 47's practice-sequence section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Evaluation Framework for ICS Cyber Incidents, The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex, Stuxnet: First Cyber-Physical Weapon; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane.
2. Frame	Answer the lens question: Which asset, architecture record, consequence, operator decision, and recovery path is being exercised defensively?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Evaluation Framework for ICS Cyber Incidents: tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the cyber-physical tabletop evidence packet fields for Evaluation Framework for ICS Cyber Incidents.	Unit profile note.	Evidence artifacts include asset-consequence map, operator decision log.
4. Challenge	Test the misconception that Evaluation Framework for ICS Cyber Incidents (ScienceDirect 2021) is optional whenever separate cyber analysis from unsafe process control or live operational action feels inconvenient.	Failure-mode note.	The artifact applies the key distinction: separate cyber analysis from unsafe process control or live operational action.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

65.2.4.1 Historical ICS Cyber Incidents: Intelligence Analysis instructor notes: source reasoning, review points, and studio focus

Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**. [252, 2026]; [255, 2026].

65.2.4.2 Historical ICS Cyber Incidents: Intelligence Analysis extension exercise: peer validation and refresh trigger review

Evidence anchor. Section 65; [252, 2026].

Have learners swap artifacts and apply the **Cyber-Physical Readiness Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**.

65.2.5 Historical ICS Cyber Incidents: Intelligence Analysis knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 65; [252, 2026].

1. Explain how **Evaluation Framework for ICS Cyber Incidents (ScienceDirect 2021)** is defined here; name the source descriptor that supports the definition.
2. Contrast **Evaluation Framework for ICS Cyber Incidents** with **The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex** using the **Cyber-Physical Readiness Lens** artifact fields.
3. Identify one failure mode from the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which cyber observation changes meaning once physical consequence is considered?
5. Correct this misconception: that Evaluation Framework for ICS Cyber Incidents (ScienceDirect 2021) is optional whenever separate cyber analysis from unsafe process control or live operational action feels inconvenient.

65.2.5.1 Historical ICS Cyber Incidents: Intelligence Analysis answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Evaluation Framework for ICS Cyber Incidents** without source evidence, uncertainty, or a safe transfer task.

65.3 Historical ICS Cyber Incidents: Intelligence Analysis assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 65; [252, 2026].

65.3.1 Historical ICS Cyber Incidents: Intelligence Analysis evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 65; [252, 2026].

65.3.2 Historical ICS Cyber Incidents: Intelligence Analysis transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 65; [252, 2026].

65.3.2.1 Historical ICS Cyber Incidents: Intelligence Analysis lineage and source tradition: profile, concepts, and first anchors

This sits in the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lineage: defensive intelligence for safety-critical environments where availability, engineering state, and physical consequence matter. [252, 2026]; [255, 2026].

65.3.2.2 Historical ICS Cyber Incidents: Intelligence Analysis working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 65; [252, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**, with provenance and reviewability throughout.

65.3.2.3 Historical ICS Cyber Incidents: Intelligence Analysis knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** synthetic process logs, asset/consequence maps, operator decisions, safety stops, and recovery evidence. [252, 2026]; [255, 2026].
- **Transforms:** asset-consequence mapping, ATT&CK-for-ICS coverage review, operator-decision rehearsal, and after-action learning.
- **Outputs:** cyber-physical tabletop packet, debrief rubric, recovery note, and control-coverage map.
- **Failure modes:** IT-first assumptions, unsafe actuation, live-control drift, and missing safety review.

65.3.2.4 Historical ICS Cyber Incidents: Intelligence Analysis transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 65; [252, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**.
- **Evidence contract:** keep the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as cyber-physical tabletop packet, debrief rubric, recovery note, and control-coverage map that another reviewer can audit.

65.3.2.5 Historical ICS Cyber Incidents: Intelligence Analysis profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 65; [252, 2026].

The matched profile emphasizes defensive intelligence for safety-critical environments where availability, engineering state, and physical consequence matter. The method stack is asset/consequence mapping, ATT&CK-for-ICS coverage review, defense-in-depth audit, remote-access check, and tabletop injects; the local topic cluster is **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**.

65.3.3 Historical ICS Cyber Incidents: Intelligence Analysis evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 65; [252, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** profile tells reviewers what evidence is strong enough for the module artifact built around **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**.

65.3.3.1 Historical ICS Cyber Incidents: Intelligence Analysis guide source spine: inherited keys and local citation roles

Primary guide citations: [252, 2026]; [255, 2026]; [270, 2026]; [279, 2026]; [282, 2026]; [284, 2026]; [289, 2026]; [291, 2026]; [296, 2026]; [217, 2026]; [218, 2026]; [219, 2026]; [220, 2026].

65.3.3.2 Historical ICS Cyber Incidents: Intelligence Analysis verified source canon: direct anchors and claim boundaries

The source canon has three tiers; the local spine begins with [252, 2026]; [255, 2026].

Tier	What counts	How it is used
Source guide	[252, 2026]; [255, 2026]; [270, 2026]; [279, 2026]; [282, 2026]; [284, 2026]; [289, 2026]; [291, 2026]; [296, 2026]; [217, 2026]; [218, 2026]; [219, 2026]; [220, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 47's source-canon section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex** and [252, 2026]; [255, 2026], but only directly verified source URLs are encoded as citations.

65.3.3.3 Historical ICS Cyber Incidents: Intelligence Analysis intelligence practice lens: evidence artifact and safety check Practice lens: **Cyber-Physical Readiness Lens** for **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**. [252, 2026]; [255, 2026].

Planning question: Which asset, architecture record, consequence, operator decision, and recovery path is being exercised defensively?

Evidence artifact: tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric.

Validation rule: validate against safety, availability, engineering state, incident scope, and after-action learning. Applied to **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**.

Handoff contract: separate cyber indicators, process observations, safety impact, operator choices, and recovery evidence.

Safety check: keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions.

65.3.3.4 Historical ICS Cyber Incidents: Intelligence Analysis runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 65; [252, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	47.99	47.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Historical ICS Cyber Incidents: Intelligence Analysis to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Bounded autonomy, procurement, incident-response, and assurance studio	47.101	47.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Historical ICS Cyber Incidents: Intelligence Analysis	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Model-card, recoverability, retention, and learner-support evidence package	47.102	47.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Historical ICS Cyber Incidents: Intelligence Analysis	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Evaluation Framework for ICS Cyber Incidents (ScienceDirect 2021)	47.1	47.1 Evaluation Framework for ICS Cyber Incidents (ScienceDirect 2021)	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex	47.2	47.2 The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Stuxnet: First Cyber-Physical Weapon — Operation Olympic Games	47.2.1	47.2.1 Stuxnet: First Cyber-Physical Weapon — Operation Olympic Games	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
BlackEnergy: Ukraine Power Grid Attacks (2015)	47.2.2	47.2.2 BlackEnergy: Ukraine Power Grid Attacks (2015)	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
CrashOverride/Industroyer: Protocol-Agnostic Power Grid Weapon	47.2.3	47.2.3 CrashOverride/Industroyer: Protocol-Agnostic Power Grid Weapon	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Triton/Trisis: Safety Instrumented System Attack	47.2.4	47.2.4 Triton/Trisis: Safety Instrumented System Attack	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Irongate: Stuxnet Descendant Against Simulated Environment	47.2.5	47.2.5 Irongate: Stuxnet Descendant Against Simulated Environment	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Havex: IT-OT Pivot Using Weaponized OPC Software	47.2.6	47.2.6 Havex: IT-OT Pivot Using Weaponized OPC Software	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Threat Scoring Framework: Malware Sophistication × Attack Consequence	47.3	47.3 Threat Scoring Framework: Malware Sophistication × Attack Consequence	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions

65.3.3.5 Historical ICS Cyber Incidents: Intelligence Analysis reusable subsection contract: topic rows, artifacts, and safety duties Evidence anchor. Section 65; [252, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Evaluation Framework for ICS Cyber Incidents (ScienceDirect 2021)	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Stuxnet: First Cyber-Physical Weapon — Operation Olympic Games	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
BlackEnergy: Ukraine Power Grid Attacks (2015)	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
CrashOverride/Industroyer: Protocol-Agnostic Power Grid Weapon	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Triton/Trisis: Safety Instrumented System Attack	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions

Lesson topic	Practice lens	Evidence artifact	Safety check
Irongate: Stuxnet Descendant Against Simulated Environment	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Havex: IT-OT Pivot Using Weaponized OPC Software	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Threat Scoring Framework: Malware Sophistication × Attack Consequence	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions

65.3.3.6 Historical ICS Cyber Incidents: Intelligence Analysis annotated source ledger: real titles and local contribution Each source cited by this **ICS/OT Cyber-Physical Defense and Tabletop Readiness** module is paired below with its real title and a one-line note on what it contributes to **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**.

Source	Cited work	What it contributes	Status
[252, 2026]	Data Act Explained	An official European Commission explainer on the EU Data Act, which became applicable on 12 September 2025.	verified source-guide
[255, 2026]	Web of Things (WoT) Architecture 1.1	The W3C Recommendation for Web of Things Architecture 1.1, published in December 2023, defining an abstract architecture for interoperability across diverse Internet of Things platforms. It introduces core concepts including Things described by machine-readable Thing Descriptions, reusable Thing Models, and Consumers that interpret descriptions to interact via Properties, Actions, and Events.	verified source-guide
[270, 2026]	NIST Big Data Interoperability Framework	NIST Special Publication 1500-1 (revised edition by Chang and Grady) establishes foundational terminology and consensus definitions for Big Data through the NIST Big Data Public Working Group. The volume defines Big Data characteristics, taxonomy, and a reference architecture assigning roles to Application Providers, Data Consumers, Data Providers, and System Orchestrators.	verified source-guide
[279, 2026]	Open Contracting Data Standard	The documentation homepage for the Open Contracting Data Standard, version 1.1.5, maintained by the Open Contracting Partnership to support disclosure of government contracting data across the procurement lifecycle. It provides a common data model spanning planning, tender, award, contract, and implementation stages, along with a primer, implementation guidance, technical schemas, and validation tooling.	verified source-guide
[282, 2026]	AI Research: Security and Resilience	A NIST page on AI research focused on security and resilience, framing these as core characteristics of trustworthy AI under the NIST AI Risk Management Framework.	verified source-guide

Source	Cited work	What it contributes	Status
[284, 2026]	Verifiable Credential Data Integrity 1.0	The W3C Recommendation for Verifiable Credential Data Integrity 1.0, published May 2025, defining mechanisms for ensuring the authenticity and integrity of verifiable credentials using cryptographic proofs. It specifies a process of data transformation, hashing, and proof generation, and a corresponding verification procedure, along with a proof data model containing properties such as type, verification method, purpose, and proof value.	verified source-guide
[289, 2026]	Guidance for Organisations Using the Algorithmic Transparency Recording Standard	This is a GOV.UK guidance page published by the Government Digital Service that instructs public sector organizations on completing the Algorithmic Transparency Recording Standard (ATRS) template and publishing their records to the GOV.UK repository. It applies both to central government bodies required to publish under mandatory policy and to other public sector bodies doing so voluntarily.	verified source-guide
[291, 2026]	Revised 508 Standards and 255 Guidelines	Official documentation from the U.S. Access Board on the Revised 508 Standards and 255 Guidelines for information and communication technology accessibility. It establishes mandatory accessibility requirements for federal agencies and voluntary guidelines for telecommunications manufacturers, covering hardware, software, websites, electronic documents, and support services.	verified source-guide
[296, 2026]	Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile	NIST AI 600-1, the Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, a cross-sectoral companion resource to the NIST AI RMF 1.0 issued pursuant to Executive Order 14110. It identifies risks that are unique to or amplified by generative AI and organizes suggested actions for managing those risks, mapped to the AI RMF functions.	verified source-guide
[217, 2026]	An evaluation framework for industrial control system cyber incidents	We analyze six significant ICS cyber incidents in the energy and power industries, namely Stuxnet.	original source-guide
[218, 2026]	THE CYBER-PHYSICAL SIX / Honeywell	An executive research report from Honeywell's Global Analysis, Research, and Defense group titled "The Cyber-Physical Six," tracing how targeted industrial attacks have evolved and predicting future trends. It reviews six landmark cyber-physical attacks affecting industrial control and operational technology systems, then analyzes observed trends such as modularity, expanding capabilities, and the increasing frequency of new attack tools.	verified source-guide
[219, 2026]	Stuxnet 15 Years Later and the Evolution of Cyber Threats to Critical	I've been asked specifically to describe how.	original source-guide

Source	Cited work	What it contributes	Status
[220, 2026]	Zetter details how Stuxnet marked a turning point in cyberwarfare	Journalist Kim Zetter testified before Congress on how Stuxnet demonstrated that physical infrastructure could be destroyed through malicious code alone, targeting Siemens programmable logic controllers at Iran's Natanz uranium enrichment facility.	verified source-guide

Where this sits. This module's overview is Section 65; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

65.3.4 Historical ICS Cyber Incidents: Intelligence Analysis governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 65; [252, 2026].

65.3.5 Historical ICS Cyber Incidents: Intelligence Analysis analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 47's governance-boundary section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **ICS/OT Cyber-Physical Defense and Tabletop Readiness** for **Evaluation Framework for ICS Cyber Incidents (ScienceDirect 2021); The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**. [252, 2026]; [255, 2026].

Curriculum topic spine: Evaluation Framework for ICS Cyber Incidents (ScienceDirect 2021), **The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**, **Stuxnet: First Cyber-Physical Weapon — Operation Olympic Games**. **Verified anchor cluster:** [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]; [Cybersecurity and Agency, 2026a]; [Cybersecurity and Agency, 2026c]; [MITRE, 2026c].

Conceptual depth: defensive intelligence for safety-critical environments where availability, engineering state, and physical consequence matter.

Method stack: asset/consequence mapping, ATT&CK-for-ICS coverage review, defense-in-depth audit, remote-access check, and tabletop injects.

Composability contract: separate cyber indicators, engineering observations, safety impacts, operator decisions, and recovery actions.

Known failure modes: IT-first assumptions, unsafe automation, untested shutdown logic, poor remote-access control, and missing after-action learning.

Defensive boundary: all ICS work remains tabletop, lab, or accountable defensive review; no exploitation, unsafe process manipulation, or live control actions. Applied to **Evaluation Framework for ICS Cyber Incidents (ScienceDirect 2021); The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**.

Anchor	Why it matters here
[of Standards and Technology, 2024f]	Official cybersecurity-risk governance framework that adds the Govern function and supplies a common language for AI, OT, and enterprise risk. Checked as of 2026-05-21; role: curriculum_anchor.
[of Standards and Technology, 2022b]	Systems-security engineering foundation for trustworthy systems in contested operational environments and related training programs. Checked as of 2026-05-21; role: curriculum_anchor.
[of Standards and Technology, 2024b]	Official NIST operational technology security guidance. Checked as of 2026-05-21; role: source_quality_anchor.
[of Automation, 2026]	Official ISA overview of industrial automation and control security standards. Checked as of 2026-05-21; role: source_quality_anchor.
[Cybersecurity and Agency, 2026a]	Official prioritized baseline of IT and OT cybersecurity practices for critical-infrastructure risk reduction and maturity assessment. Checked as of 2026-05-21; role: curriculum_anchor.
[Cybersecurity and Agency, 2026c]	Official defensive ICS practice library for defense-in-depth, forensics, incident response, and remote access. Checked as of 2026-05-21; role: curriculum_anchor.
[MITRE, 2026c]	Threat-informed defensive matrix for ICS tactics and techniques, used for coverage mapping. Checked as of 2026-05-21; role: curriculum_anchor.

65.3.5.1 Historical ICS Cyber Incidents: Intelligence Analysis evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [252, 2026]; [255, 2026].

65.3.6 Historical ICS Cyber Incidents: Intelligence Analysis agentic boundary: assist, approve, block, and record

Evidence anchor. Section 65; [252, 2026].

AGEINT translation is bounded by the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**.

65.3.6.1 Historical ICS Cyber Incidents: Intelligence Analysis permitted defensive utility: curriculum uses and safe outputs

Evidence anchor. Section 65; [252, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**.

65.3.6.2 Historical ICS Cyber Incidents: Intelligence Analysis excluded operational boundary: blocked actions and stop rules

Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [252, 2026]; [255, 2026] and **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

65.3.7 Historical ICS Cyber Incidents: Intelligence Analysis governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 65; [252, 2026].

Governance is practiced as a gate on the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane. Learners use the **Cyber-Physical Readiness Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**.

65.3.7.1 Historical ICS Cyber Incidents: Intelligence Analysis governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [252, 2026]; [255, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **ICS/OT Cyber-Physical Defense and Tabletop Readiness** failure modes and the **Cyber-Physical Readiness Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

65.3.7.2 Historical ICS Cyber Incidents: Intelligence Analysis evidence package handoff: appendices, records, and reuse Evidence anchor. Section 65; [252, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Cyber-Physical Readiness Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**.

65.3.7.3 Historical ICS Cyber Incidents: Intelligence Analysis current-source assurance: verified anchors and local artifact fit The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**. [252, 2026]; [255, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_nist_csf_2` for **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**?	The NIST Cybersecurity Framework (CSF) 2.0; lane `ics_ot_defense`; checked 2026-05-21.	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric; Official cybersecurity-risk governance framework that adds the Govern function and supplies a common language for AI, OT, and enterprise risk.
What does the module inherit from `official_nist_sp_800_160r1` for **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**?	Engineering Trustworthy Secure Systems, NIST SP 800-160 Vol. 1 Rev. 1; lane `ics_ot_defense`; checked 2026-05-21.	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric; Systems-security engineering foundation for trustworthy systems in contested operational environments and related training programs.
What does the module inherit from `official_nist_sp_800_82r3` for **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**?	Guide to Operational Technology Security, NIST SP 800-82 Rev. 3; lane `source_quality_spine`; checked 2026-05-21.	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric; Official NIST operational technology security guidance.
What does the module inherit from `official_isa_iec_62443` for **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**?	ISA/IEC 62443 Series of Standards; lane `source_quality_spine`; checked 2026-05-21.	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric; Official ISA overview of industrial automation and control security standards.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 65; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

65.3.8 Historical ICS Cyber Incidents: Intelligence Analysis assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 65; [252, 2026].

65.3.9 Historical ICS Cyber Incidents: Intelligence Analysis assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 65; [252, 2026].

65.3.9.1 Historical ICS Cyber Incidents: Intelligence Analysis capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**.
Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex** and [252, 2026]; [255, 2026].

65.3.9.2 Historical ICS Cyber Incidents: Intelligence Analysis instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex** and [252, 2026]; [255, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

65.3.9.3 Historical ICS Cyber Incidents: Intelligence Analysis assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Evaluation Framework for ICS Cyber Incidents (ScienceDirect 2021)	Completed **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex	Completed **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Stuxnet: First Cyber-Physical Weapon — Operation Olympic Games	Completed **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

65.3.10 Historical ICS Cyber Incidents: Intelligence Analysis refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [252, 2026]; [255, 2026] and **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**.

65.3.10.1 Historical ICS Cyber Incidents: Intelligence Analysis refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**. The local signals begin with [252, 2026]; [255, 2026].

65.3.10.2 Historical ICS Cyber Incidents: Intelligence Analysis claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**, and the source spine for these checks begins with [252, 2026]; [255, 2026].

65.3.11 Historical ICS Cyber Incidents: Intelligence Analysis reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [252, 2026]; [255, 2026].
Triangulation anchors. In module 47's review-checklist section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex**. [252, 2026]; [255, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.

- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

65.3.12 Historical ICS Cyber Incidents: Intelligence Analysis learning-path links: module map, overview, and curriculum atlas

Use the cross-links below to place **Evaluation Framework for ICS Cyber Incidents; The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex** in the wider unit: the orientation sets the frame, the parent unit supplies the shared safety posture, and the neighbouring modules show what evidence enters and leaves. Lead sources: [252, 2026]; [255, 2026].
Section 2, Section 62, Section 64, Section 66

66 Threat Intelligence Sharing for Critical Infrastructure

66.0.1 Threat Intelligence Sharing for Critical Infrastructure figures and course links: visual evidence, source flow, and navigation

The module uses Figure 140 and Figure 134 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.

Navigation links: Section 2, Section 62, Section 65, Section 67.

This module teaches the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane through a bounded, source-backed coursebook chapter. [253, 2026]; [258, 2026].

66.1 ICS/OT Cyber-Physical Defense and Tabletop Readiness frame for Threat Intelligence Sharing for Critical Infrastructure: source context, topic focus, and reader task

Evidence anchor. Section 66; [253, 2026].

66.1.1 Threat Intelligence Sharing for Critical Infrastructure orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 66; [253, 2026].

66.1.2 Threat Intelligence Sharing for Critical Infrastructure conceptual primer: source context, core model, and reader task

This chapter teaches ICS/OT intelligence as safety-aware defensive reasoning: asset state, engineering consequence, operator decision, and recovery evidence matter as much as cyber indicators. The chapter uses **Cyber-Physical Readiness Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC**.

The central distinction is to separate cyber analysis from unsafe process control or live operational action. Core topics include **Evidence-Driven Analysis of Threat Information Sharing for ICS (arXiv 2025); ISACs: E-ISAC, WaterISAC, FS-ISAC; CISA Frameworks for Critical Infrastructure**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.

Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [253, 2026]; [258, 2026].

Learners move from vocabulary and the **Cyber-Physical Readiness Lens** distinction through topic lessons on **Evidence-Driven Analysis of Threat Information Sharing for ICS (arXiv 2025)** with evidence and misconception checks, then assemble a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** with safety and rights gates.

66.1.3 Threat Intelligence Sharing for Critical Infrastructure learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 66; [253, 2026].

- Connect **Evidence-Driven Analysis of Threat Information Sharing for ICS (arXiv 2025) and ISACs: E-ISAC, WaterISAC, FS-ISAC** to **ICS/OT Cyber-Physical Defense and Tabletop Readiness** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate cyber analysis from unsafe process control or live operational action; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as IT-first assumptions, unsafe automation, untested shutdown logic, poor remote-access control, and missing after-action learning, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: all ICS work remains tabletop, lab, or accountable defensive review; no exploitation, unsafe process manipulation, or live control actions.

66.1.4 Threat Intelligence Sharing for Critical Infrastructure core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 66; [253, 2026].

Term	Working definition
Engineering state	the physical or process condition that gives cyber evidence safety meaning
Consequence	the operational, safety, environmental, or service effect of a condition
Defense in depth	layered prevention, detection, response, and recovery controls
Tabletop inject	a synthetic event used to rehearse decisions without touching live systems
Recovery evidence	proof that a safe state, service, or learning objective was restored
Evidence-Driven Analysis of Threat Information…	Key terms: Evidence, Driven, Analysis.
ISACs: E-ISAC, WaterISAC, FS-ISAC	Key terms: ISACs, ISAC, WaterISAC.

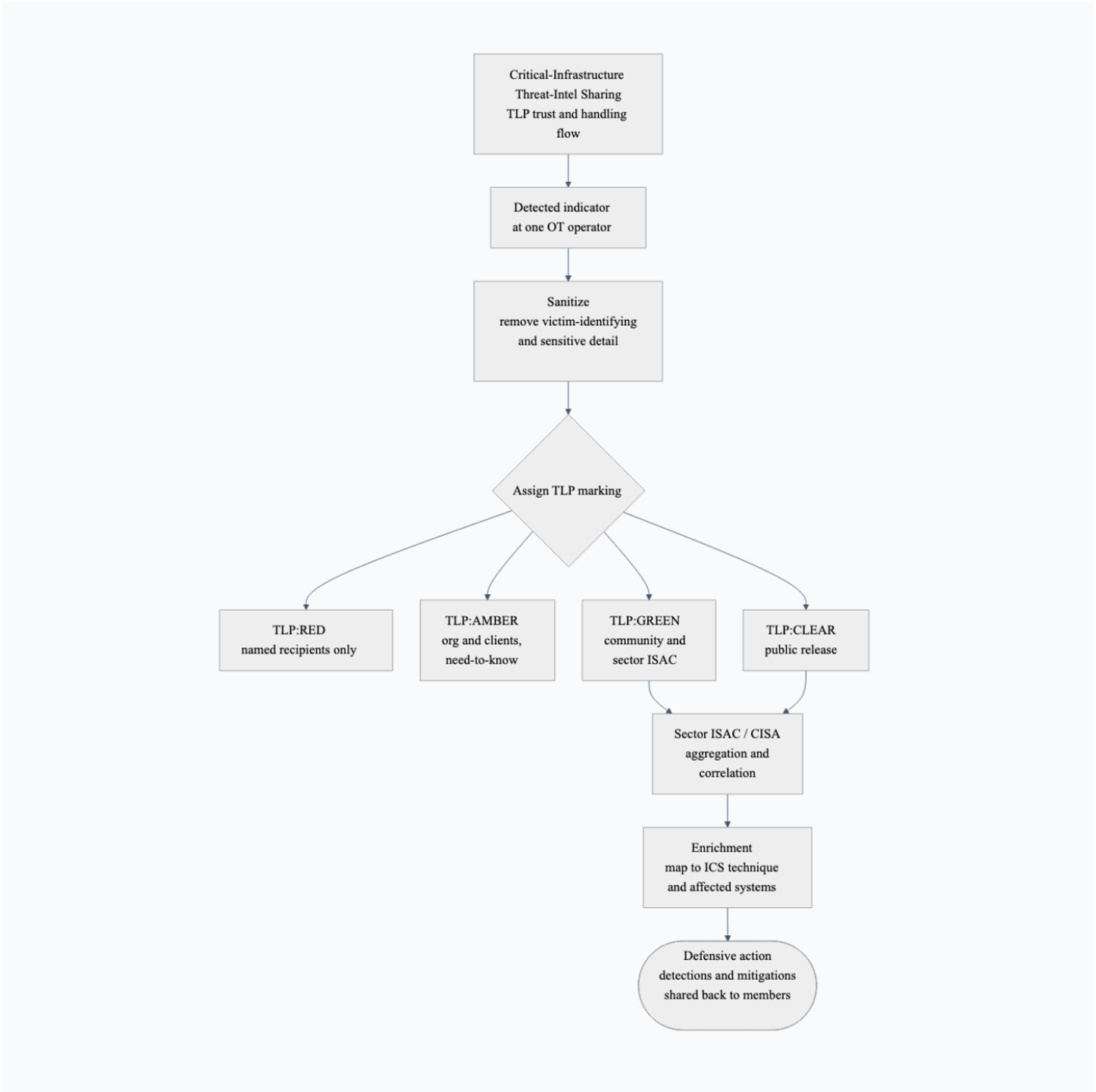


Figure 140: This diagram teaches how a detected indicator is sanitized, marked with a Traffic Light Protocol level, and routed through a sector ISAC so defensive mitigations flow back to the community. It is anchored to the industrial and cyber physical intelligence / threat intelligence sharing for critical infrastructure section; use it to inspect Critical-Infrastructure Threat-Intel Sharing TLP trust and handling flow, Detected indicator at one OT operator, Sanitize remove victim-identifying and sensitive detail, and TLP:RED named recipients only while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

66.2 Cyber-Physical Readiness Lens path for Threat Intelligence Sharing for Critical Infrastructure: lesson cluster, safe artifact, and review

Evidence anchor. Section 66; [253, 2026].

66.2.1 Threat Intelligence Sharing for Critical Infrastructure practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 66; [253, 2026].

66.2.2 Threat Intelligence Sharing for Critical Infrastructure topic lessons: source-backed concepts and transfer tasks

This module builds ICS/OT intelligence as safety-aware defensive reasoning: asset state, engineering consequence, operator decision, and recovery evidence matter as much as cyber indicators. The sequence opens with **Evidence-Driven Analysis of Threat Information Sharing for ICS (arXiv 2025)**, **ISACs: E-ISAC, WaterISAC, FS-ISAC**, **CISA Frameworks for Critical Infrastructure** and applies the **Cyber-Physical Readiness Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 134; module overview Section 66; curriculum atlas Section 2.

Triangulation anchors. In module 48's topic-lessons section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

66.2.2.1 Lesson 1: Evidence-Driven Analysis of Threat Information Sharing for ICS (arXiv 2025) Concept. Evidence-Driven Analysis of Threat Information Sharing for ICS (arXiv 2025) evaluates ISAC sharing by handling rules, anonymization, confidence, and consumer responsibilities.

Why it matters. Analysts use **Evidence-Driven Analysis** to separate cyber analysis from unsafe process control or live operational action. A defensible treatment names the judgment it enables for safety-aware tabletop readiness and defensive coverage review, the proof limit that IT-first assumptions would otherwise hide, and the reviewer accountable for challenge.

Source support. Evidence-Driven Analysis of Threat Information Sharing for ICS (arXiv 2025) rests on [077, 2026]. The most specific cited work observes: Drawing on three major ICS attacks and a review of 196 procedure examples across 22 malware families, it identifies limitations including incomplete support in the STIX sharing standard, reliance on proprietary undocumented protocols, and insufficient technical detail in threat and vulnerability reports. Use it for the working definition that **Evidence-Driven Analysis of Threat Information Sharing for ICS (arXiv 2025)** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. Ground **Evidence-Driven Analysis** in the evidence the row cites. [077, 2026] An arXiv research paper presenting an evidence-driven analysis of why threat information sharing for industrial control systems remains ineffective. Drawing on three major ICS attacks and a review of 196 procedure examples across 22 malware families, it identifies limitations including incomplete support in the STIX sharing standard, reliance on proprietary undocumented protocols, and insufficient technical detail in threat and vulnerability reports. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Evidence-Driven Analysis**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must state the handling descriptor, the bounded claim about **Evidence-Driven Analysis of Threat Information**, the anonymization caveat, the confidence note, the consumer-duty boundary, and the reviewer who clears sharing. Shape **Evidence-Driven Analysis** work as a **cyber-physical tabletop evidence packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Evidence-Driven Analysis**: that information being shareable for defense means it carries no sensitivity, attribution, or need-to-know limits on who receives it.

Transfer task. Transfer **Evidence-Driven Analysis** from this module to a second motif by preserving safety-aware tabletop readiness and defensive coverage review, replacing action with audit, and naming the blocked use.

66.2.2.2 Lesson 2: ISACs: E-ISAC, WaterISAC, FS-ISAC Concept. ISACs: E-ISAC, WaterISAC, FS-ISAC evaluates ISAC sharing by handling rules, anonymization, confidence, and consumer responsibilities.

Why it matters. Without explicit treatment of **ISACs: E-ISAC, WaterISAC, FS-ISAC**, IT-first assumptions undermines safety-aware tabletop readiness and defensive coverage review; the lesson builds the habit to separate cyber analysis from unsafe process control or live operational action.

Source support. ISACs: E-ISAC, WaterISAC, FS-ISAC rests on [307, 2026], [305, 2026], and [304, 2026]. The closest source to this row notes: NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Use them for pinning down the scope of **ISACs: E-ISAC, WaterISAC, FS-ISAC**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. For **ISACs: E-ISAC, WaterISAC, FS-ISAC**, work from the cited evidence behind this row. [307, 2026] Official CISA Industrial Control Systems recommended practices page for defensive ICS/OT safety, resilience, and incident-preparation guidance. [305, 2026] Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **ISACs**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must state the handling descriptor, the bounded claim about **ISACs**, the anonymization caveat, the confidence note, the consumer-duty boundary, and the reviewer who clears sharing. Shape **ISACs: E-ISAC, WaterISAC, FS-ISAC** work as a **cyber-physical tabletop evidence packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **ISACs: E-ISAC, WaterISAC, FS-ISAC**: that information being shareable for defense means it carries no sensitivity, attribution, or need-to-know limits on who receives it.

Transfer task. Apply this module's safe boundary for **ISACs: E-ISAC, WaterISAC, FS-ISAC** to another artifact while keeping safety-aware tabletop readiness and defensive coverage review and reviewer ownership explicit.

66.2.2.3 Lesson 3: CISA Frameworks for Critical Infrastructure Concept. CISA Frameworks for Critical Infrastructure evaluates ISAC sharing by handling rules, anonymization, confidence, and consumer responsibilities.

Why it matters. Analysts use **CISA Frameworks** to separate cyber analysis from unsafe process control or live operational action. A defensible treatment names the judgment it enables for safety-aware tabletop readiness and defensive coverage review, the proof limit that IT-first assumptions would otherwise hide, and the reviewer accountable for challenge.

Source support. CISA Frameworks for Critical Infrastructure rests on [307, 2026], [305, 2026], and [304, 2026]. The lead source's own note reads: NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Use them for the working definition that **CISA Frameworks for Critical Infrastructure** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. For **CISA Frameworks**, work from the cited evidence behind this row. [307, 2026] Official CISA Industrial Control Systems recommended practices page for defensive ICS/OT safety, resilience, and incident-preparation guidance. [305, 2026] Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. Build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must state the handling descriptor, the bounded claim about **CISA Frameworks**, the anonymization caveat, the confidence note, the consumer-duty boundary, and the reviewer who clears sharing. Shape this subject work as a **cyber-physical tabletop evidence packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **CISA Frameworks**: that information being shareable for defense means it carries no sensitivity, attribution, or need-to-know limits on who receives it.

Transfer task. Reuse the **CISA Frameworks** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

66.2.2.4 Lesson 4: NERC CIP Standards

Concept. NERC CIP Standards connects NERC CIP requirements to asset inventory, access control, and audit evidence—not operational bypass.

Why it matters. NERC CIP Standards matters in the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane because safety-aware tabletop readiness and defensive coverage evidence must stay separate from judgment; IT-first assumptions is a common failure.

Source support. NERC CIP Standards rests on [307, 2026], [305, 2026], and [304, 2026]. The closest source to this row notes: NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Use them for fixing what **NERC CIP Standards** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. Read **NERC CIP Standards** against the works cited for this row. [307, 2026] Official CISA Industrial Control Systems recommended practices page for defensive ICS/OT safety, resilience, and incident-preparation guidance. [305, 2026] Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. Build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must state the handling descriptor, the bounded claim about **NERC CIP Standards**, the anonymization caveat, the confidence note, the consumer-duty boundary, and the reviewer who clears sharing. Shape this subject work as a **cyber-physical tabletop evidence packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **NERC CIP Standards**: that information being shareable for defense means it carries no sensitivity, attribution, or need-to-know limits on who receives it.

Transfer task. Apply this module's safe boundary for **NERC CIP Standards** to another artifact while keeping safety-aware tabletop readiness and defensive coverage review and reviewer ownership explicit.

66.2.2.5 Lesson 5: IDS/IPS for OT Networks: Dragos, Claroty, Nozomi, Armis

Concept. IDS/IPS for OT Networks: Dragos, Claroty, Nozomi, Armis evaluates ISAC and sector sharing by handling rules, anonymization, confidence, and consumer responsibilities.

Why it matters. IDS/IPS for OT Networks: Dragos, Claroty, Nozomi, Armis connects classroom vocabulary to ICS/OT Cyber-Physical Defense and Tabletop Readiness practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. IDS/IPS for OT Networks: Dragos, Claroty, Nozomi, Armis rests on [307, 2026], [305, 2026], and [304, 2026]. The most specific cited work observes: NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Use them for pinning down the scope of **IDS/IPS for OT Networks: Dragos, Claroty, Nozomi, Armis**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. For **IDS/IPS for OT Networks: Dragos, Claroty, Nozomi, Armis**, reason from the sources cited in this row. [307, 2026] Official CISA Industrial Control Systems recommended practices page for defensive ICS/OT safety, resilience, and incident-preparation guidance. [305, 2026] Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **IDS/IPS for OT Networks**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must state the handling descriptor, the bounded claim about **IDS/IPS for OT Networks**, the anonymization caveat, the confidence note, the consumer-duty boundary, and the reviewer who clears sharing. Shape **IDS/IPS for OT Networks: Dragos, Claroty, Nozomi, Armis** work as a **cyber-physical tabletop evidence packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **IDS/IPS for OT Networks: Dragos, Claroty, Nozomi, Armis**: that information being shareable for defense means it carries no sensitivity, attribution, or need-to-know limits on who receives it.

Transfer task. Apply this module's safe boundary for **IDS/IPS for OT Networks: Dragos, Claroty, Nozomi, Armis** to another artifact while keeping safety-aware tabletop readiness and defensive coverage review and reviewer ownership explicit.

66.2.2.6 Lesson 6: Honeywell ICS Security: Defense in Depth Concept. Honeywell ICS Security: Defense in Depth evaluates ISAC and sector sharing by handling rules, anonymization, confidence, and consumer responsibilities.

Why it matters. Without explicit treatment of **Honeywell ICS Security**, IT-first assumptions undermines safety-aware tabletop readiness and defensive coverage review; the lesson builds the habit to separate cyber analysis from unsafe process control or live operational action.

Source support. Honeywell ICS Security: Defense in Depth rests on [218, 2026]. Its anchor reference records: An executive research report from Honeywell's Global Analysis, Research, and Defense group titled "The Cyber-Physical Six," tracing how targeted industrial attacks have evolved and predicting future trends. Use it for the working definition that **Honeywell ICS Security: Defense in Depth** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. For **Honeywell ICS Security**, work from the cited evidence behind this row. [218, 2026] An executive research report from Honeywell's Global Analysis, Research, and Defense group titled "The Cyber-Physical Six," tracing how targeted industrial attacks have evolved and predicting future trends. It reviews six landmark cyber-physical attacks affecting industrial control and operational technology systems, then analyzes observed trends such as modularity, expanding capabilities, and the increasing frequency of new attack tools. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Honeywell ICS Security**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must state the handling descriptor, the bounded claim about **Honeywell ICS Security**, the anonymization caveat, the confidence note, the consumer-duty boundary, and the reviewer who clears sharing. Shape **Honeywell ICS Security** work as a **cyber-physical tabletop evidence packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **Honeywell ICS Security**: that information being shareable for defense means it carries no sensitivity, attribution, or need-to-know limits on who receives it.

Transfer task. Apply this module's safe boundary for **Honeywell ICS Security** to another artifact while keeping safety-aware tabletop readiness and defensive coverage review and reviewer ownership explicit.

66.2.3 Threat Intelligence Sharing for Critical Infrastructure worked safe example: synthetic inputs, evidence, and review

Worked example: a sample water-utility tabletop reviews synthetic process logs after a simulated anomaly. [253, 2026]; [258, 2026].

Triangulation anchors. In module 48's worked-example section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **safety-aware ICS and OT intelligence**. Learners use a **cyber-physical tabletop evidence packet** and keep this boundary visible: No live device control, unsafe process change, exploit sequence, evasion, or operational response.

Frame. The classroom question centers on **Evidence-Driven Analysis of Threat Information Sharing for ICS (arXiv 2025)**. Excluded actions stay explicit, and the **Cyber-Physical Readiness Lens** planning question is: Which asset, architecture record, consequence, operator decision, and recovery path is being exercised defensively?

Inputs. For the **Evidence-Driven Analysis of Threat Information Sharing for ICS** scenario, use toy HMI screenshots, fabricated network alerts, public ICS control guidance, and a safety stop card. The Cyber-Physical Readiness Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Evidence-Driven Analysis of Threat Information Sharing for ICS**, students map assets to consequences, classify tabletop injects, identify human decisions, and preserve recovery evidence. Pause whenever an inference about Evidence-Driven Analysis of Threat Information Sharing for ICS appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Evidence-Driven Analysis of Threat Information Sharing for ICS** classroom scenario; unit artifact = cyber-physical tabletop evidence packet; evidence = allowed inputs; method = safety-aware tabletop readiness and defensive coverage review; output = a cyber-physical tabletop packet with assets, consequences, ATT&CK mapping, decisions, and debrief; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Evidence-Driven Analysis of Threat Information Sharing for ICS** as "Cyber-Physical Readiness Lens confirms it" is not enough. The revision ties the claim to safety-aware tabletop readiness and defensive coverage review, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Evidence-Driven Analysis of Threat Information Sharing for ICS** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

66.2.4 Threat Intelligence Sharing for Critical Infrastructure practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Cyber-Physical Readiness Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC**.

Triangulation anchors. In module 48's practice-sequence section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Evidence-Driven Analysis of Threat Information Sharing for ICS, ISACs: E-ISAC, WaterISAC, FS-ISAC, CISA Frameworks for Critical Infrastructure; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane.
2. Frame	Answer the lens question: Which asset, architecture record, consequence, operator decision, and recovery path is being exercised defensively?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.

Move	Learner action	Output	Check
3. Evidence	Fill the artifact fields for Evidence-Driven Analysis of Threat Information Sharing for ICS: tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the cyber-physical tabletop evidence packet fields for Evidence-Driven Analysis of Threat Information Sharing for ICS.	Unit profile note.	Evidence artifacts include asset-consequence map, operator decision log.
4. Challenge	Test the misconception that information being shareable for defense means it carries no sensitivity, attribution, or need-to-know limits on who receives it.	Failure-mode note.	The artifact applies the key distinction: separate cyber analysis from unsafe process control or live operational action.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

66.2.4.1 Threat Intelligence Sharing for Critical Infrastructure instructor notes: source reasoning, review points, and studio focus Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC**. [253, 2026]; [258, 2026].

66.2.4.2 Threat Intelligence Sharing for Critical Infrastructure extension exercise: peer validation and refresh trigger review Evidence anchor. Section 66; [253, 2026].

Have learners swap artifacts and apply the **Cyber-Physical Readiness Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC**.

66.2.5 Threat Intelligence Sharing for Critical Infrastructure knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 66; [253, 2026].

1. Explain how **Evidence-Driven Analysis of Threat Information Sharing for ICS (arXiv 2025)** is defined here; name the source descriptor that supports the definition.
2. Contrast **Evidence-Driven Analysis of Threat Information Sharing for ICS** with **ISACs: E-ISAC, WaterISAC, FS-ISAC** using the **Cyber-Physical Readiness Lens** artifact fields.
3. Identify one failure mode from the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which cyber observation changes meaning once physical consequence is considered?
5. Correct this misconception: that information being shareable for defense means it carries no sensitivity, attribution, or need-to-know limits on who receives it.

66.2.5.1 Threat Intelligence Sharing for Critical Infrastructure answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Evidence-Driven Analysis of Threat Information Sharing for ICS** without source evidence, uncertainty, or a safe transfer task.

66.3 Threat Intelligence Sharing for Critical Infrastructure assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 66; [253, 2026].

66.3.1 Threat Intelligence Sharing for Critical Infrastructure evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 66; [253, 2026].

66.3.2 Threat Intelligence Sharing for Critical Infrastructure transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 66; [253, 2026].

66.3.2.1 Threat Intelligence Sharing for Critical Infrastructure lineage and source tradition: profile, concepts, and first anchors

This sits in the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lineage: defensive intelligence for safety-critical environments where availability, engineering state, and physical consequence matter. [253, 2026]; [258, 2026].

66.3.2.2 Threat Intelligence Sharing for Critical Infrastructure working model: inputs, constraints, transforms, outputs, and oversight

Evidence anchor. Section 66; [253, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC**, with provenance and reviewability throughout.

66.3.2.3 Threat Intelligence Sharing for Critical Infrastructure knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** synthetic process logs, asset/consequence maps, operator decisions, safety stops, and recovery evidence. [253, 2026]; [258, 2026].
- **Transforms:** asset-consequence mapping, ATT&CK-for-ICS coverage review, operator-decision rehearsal, and after-action learning.
- **Outputs:** cyber-physical tabletop packet, debrief rubric, recovery note, and control-coverage map.
- **Failure modes:** IT-first assumptions, unsafe actuation, live-control drift, and missing safety review.

66.3.2.4 Threat Intelligence Sharing for Critical Infrastructure transfer contracts: authority, evidence, tools, and auditable output

Evidence anchor. Section 66; [253, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC**.
- **Evidence contract:** keep the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as cyber-physical tabletop packet, debrief rubric, recovery note, and control-coverage map that another reviewer can audit.

66.3.2.5 Threat Intelligence Sharing for Critical Infrastructure profile emphasis and local focus: method stack and topic cluster

Evidence anchor. Section 66; [253, 2026].

The matched profile emphasizes defensive intelligence for safety-critical environments where availability, engineering state, and physical consequence matter. The method stack is asset/consequence mapping, ATT&CK-for-ICS coverage review, defense-in-depth audit, remote-access check, and tabletop injects; the local topic cluster is **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC**.

66.3.3 Threat Intelligence Sharing for Critical Infrastructure evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 66; [253, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** profile tells reviewers what evidence is strong enough for the module artifact built around **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC**.

66.3.3.1 Threat Intelligence Sharing for Critical Infrastructure guide source spine: inherited keys and local citation roles

Primary guide citations: [253, 2026]; [258, 2026]; [261, 2026]; [275, 2026]; [276, 2026]; [283, 2026]; [286, 2026]; [293, 2026]; [295, 2026]; [077, 2026]; [218, 2026]; [307, 2026]; [305, 2026]; [304, 2026].

66.3.3.2 Threat Intelligence Sharing for Critical Infrastructure verified source canon: direct anchors and claim boundaries

The source canon has three tiers; the local spine begins with [253, 2026]; [258, 2026].

Tier	What counts	How it is used
Source guide	[253, 2026]; [258, 2026]; [261, 2026]; [275, 2026]; [276, 2026]; [283, 2026]; [286, 2026]; [293, 2026]; [295, 2026]; [077, 2026]; [218, 2026]; [307, 2026]; [305, 2026]; [304, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 48's source-canon section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC** and [253, 2026]; [258, 2026], but only directly verified source URLs are encoded as citations.

66.3.3.3 Threat Intelligence Sharing for Critical Infrastructure intelligence practice lens: evidence artifact and safety check Practice lens: **Cyber-Physical Readiness Lens** for **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC**. [253, 2026]; [258, 2026].

Planning question: Which asset, architecture record, consequence, operator decision, and recovery path is being exercised defensively?

Evidence artifact: tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric.

Validation rule: validate against safety, availability, engineering state, incident scope, and after-action learning. Applied to **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC**.

Handoff contract: separate cyber indicators, process observations, safety impact, operator choices, and recovery evidence.

Safety check: keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions.

66.3.3.4 Threat Intelligence Sharing for Critical Infrastructure runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 66; [253, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	48.99	48.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Threat Intelligence Sharing for Critical Infrastructure to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Bounded autonomy, procurement, incident-response, and assurance studio	48.101	48.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Threat Intelligence Sharing for Critical Infrastructure	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Model-card, recoverability, retention, and learner-support evidence package	48.102	48.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Threat Intelligence Sharing for Critical Infrastructure	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Evidence-Driven Analysis of Threat Information Sharing for ICS (arXiv 2025)	48.1	48.1 Evidence-Driven Analysis of Threat Information Sharing for ICS (arXiv 2025)	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
ISACs: E-ISAC, WaterISAC, FS-ISAC	48.2	48.2 ISACs: E-ISAC, WaterISAC, FS-ISAC	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
CISA Frameworks for Critical Infrastructure	48.3	48.3 CISA Frameworks for Critical Infrastructure	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
NERC CIP Standards	48.4	48.4 NERC CIP Standards	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
IDS/IPS for OT Networks: Dragos, Claroty, Nozomi, Armis	48.5	48.5 IDS/IPS for OT Networks: Dragos, Claroty, Nozomi, Armis	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Honeywell ICS Security: Defense in Depth	48.6	48.6 Honeywell ICS Security: Defense in Depth	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions

66.3.3.5 Threat Intelligence Sharing for Critical Infrastructure reusable subsection contract: topic rows, artifacts, and safety duties Evidence anchor. Section 66; [253, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Evidence-Driven Analysis of Threat Information Sharing for ICS (arXiv 2025)	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
ISACs: E-ISAC, WaterISAC, FS-ISAC	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
CISA Frameworks for Critical Infrastructure	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
NERC CIP Standards	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
IDS/IPS for OT Networks: Dragos, Claroty, Nozomi, Armis	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Honeywell ICS Security: Defense in Depth	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions

66.3.3.6 Threat Intelligence Sharing for Critical Infrastructure annotated source ledger: real titles and local contribution Each source cited by this **ICS/OT Cyber-Physical Defense and Tabletop Readiness** module is paired below with its real title and a one-line note on what it contributes to **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC**.

Source	Cited work	What it contributes	Status
[253, 2026]	Common European Data Spaces	This is an official European Commission webpage describing the Common European Data Spaces initiative, part of the EU strategy to create interconnected, trustworthy data-sharing environments across strategic sectors. It explains that data spaces let organizations and individuals share data while retaining control, guided by principles of open participation, privacy protection, and fair access rules.	verified source-guide
[258, 2026]	OpenAPI Specification	The official OpenAPI Initiative publications page, serving as a central index for the OpenAPI Specification and related standards including the Arazzo and Overlay specifications. It provides access to multiple specification versions (2.0, 3.0, 3.1, and 3.2) and their corresponding downloadable schemas identified by release date, along with a registry of extensions, formats, media types, and other resources.	verified source-guide
[261, 2026]	RFC 9110: HTTP Semantics	RFC 9110, the official IETF standards document defining the core semantics and architecture of HTTP, published in June 2022 and consolidating nine earlier RFCs. It establishes terminology and protocol aspects shared across HTTP versions, including methods, status codes, header fields, content negotiation, conditional and range requests, authentication, and the http and https URI schemes.	verified source-guide
[275, 2026]	Fact Sheet: New Rule on the Accessibility of Web Content and Mobile Apps Provided by State and Local Governments	A US Department of Justice fact sheet explaining the 2024 ADA Title II rule requiring state and local governments to make their web content and mobile apps accessible. It establishes WCAG 2.1 Level AA as the technical standard, applies to entities such as schools, courts, libraries, and transit agencies, and sets compliance deadlines of April 2027 for larger jurisdictions and April 2028 for smaller ones.	verified source-guide
[276, 2026]	What is a Data Protection Impact Assessment and When Is This Mandatory?	A European Data Protection Board FAQ page, part of its data protection guide for small businesses, explaining Data Protection Impact Assessments (DPIAs) and when they are mandatory. It describes a DPIA as a written assessment of the impact of a planned processing operation, required when processing poses high risks to individuals' rights.	verified source-guide
[283, 2026]	Recommendation of the Council on Open Government	An OECD legal instrument document reproducing the Recommendation of the Council on Open Government (OECD/LEGAL/0438), adopted on 14 December 2017. It defines open government as a culture of governance promoting transparency, integrity, accountability, and stakeholder participation in support of democracy and inclusive growth.	verified source-guide

Source	Cited work	What it contributes	Status
[286, 2026]	Model Cards for Model Reporting	The arXiv abstract for "Model Cards for Model Reporting" (2018) by Mitchell, Wu, Zaldivar, and colleagues, which introduces a framework for transparent documentation of machine learning models. Model cards are short accompanying documents that report a model's benchmarked performance across varied conditions, including different cultural, demographic, and phenotypic groups, along with intended use, evaluation methodology, and deployment considerations.	verified source-guide
[293, 2026]	Inventory of NARA Artificial Intelligence (AI) Use Cases	The National Archives and Records Administration (NARA) official inventory of its artificial intelligence use cases, documenting 14 projects across deployed, pilot, and planned stages. Deployed efforts include workplace productivity tools, automated tagging for museum experiences, and historical record retrieval, while pilots cover PII detection and redaction, semantic search, and metadata generation, and planned work targets FOIA processing and public search.	verified source-guide
[295, 2026]	M-25-22: Driving Efficient Acquisition of Artificial Intelligence in Government	OMB Memorandum M-25-22 (April 3, 2025), Driving Efficient Acquisition of Artificial Intelligence in Government, issued under Executive Order 13960 and related directives. It provides guidance to federal agencies for acquiring effective and trustworthy AI in a timely, cost-effective manner, and rescinds and replaces earlier memorandum M-24-18.	verified source-guide
[077, 2026]	An Evidence-Driven Analysis of Threat Information Sharing	An arXiv research paper presenting an evidence-driven analysis of why threat information sharing for industrial control systems remains ineffective. Drawing on three major ICS attacks and a review of 196 procedure examples across 22 malware families, it identifies limitations including incomplete support in the STIX sharing standard, reliance on proprietary undocumented protocols, and insufficient technical detail in threat and vulnerability reports.	verified source-guide
[218, 2026]	THE CYBER-PHYSICAL SIX / Honeywell	An executive research report from Honeywell's Global Analysis, Research, and Defense group titled "The Cyber-Physical Six," tracing how targeted industrial attacks have evolved and predicting future trends. It reviews six landmark cyber-physical attacks affecting industrial control and operational technology systems, then analyzes observed trends such as modularity, expanding capabilities, and the increasing frequency of new attack tools.	verified source-guide
[307, 2026]	ICS Recommended Practices	Official CISA Industrial Control Systems recommended practices page for defensive ICS/OT safety, resilience, and incident-preparation guidance.	original source-guide
[305, 2026]	DevSecOps	Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support.	original source-guide

Source	Cited work	What it contributes	Status
[304, 2026]	Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities	NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences.	verified source-guide

Where this sits. This module's overview is Section 66; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

66.3.4 Threat Intelligence Sharing for Critical Infrastructure governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 66; [253, 2026].

66.3.5 Threat Intelligence Sharing for Critical Infrastructure analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 48's governance-boundary section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **ICS/OT Cyber-Physical Defense and Tabletop Readiness** for **Evidence-Driven Analysis of Threat Information Sharing for ICS (arXiv 2025); ISACs: E-ISAC, WaterISAC, FS-ISAC**. [253, 2026]; [258, 2026].

Curriculum topic spine: Evidence-Driven Analysis of Threat Information Sharing for ICS (arXiv 2025), ISACs: E-ISAC, WaterISAC, FS-ISAC, CISA Frameworks for Critical Infrastructure. Verified anchor cluster: [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]; [Cybersecurity and Agency, 2026a]; [Cybersecurity and Agency, 2026c]; [MITRE, 2026c].

Conceptual depth: defensive intelligence for safety-critical environments where availability, engineering state, and physical consequence matter.

Method stack: asset/consequence mapping, ATT&CK-for-ICS coverage review, defense-in-depth audit, remote-access check, and tabletop injects.

Composability contract: separate cyber indicators, engineering observations, safety impacts, operator decisions, and recovery actions.

Known failure modes: IT-first assumptions, unsafe automation, untested shutdown logic, poor remote-access control, and missing after-action learning.

Defensive boundary: all ICS work remains tabletop, lab, or accountable defensive review; no exploitation, unsafe process manipulation, or live control actions. Applied to **Evidence-Driven Analysis of Threat Information Sharing for ICS (arXiv 2025); ISACs: E-ISAC, WaterISAC, FS-ISAC**.

Anchor	Why it matters here
[of Standards and Technology, 2024f]	Official cybersecurity-risk governance framework that adds the Govern function and supplies a common language for AI, OT, and enterprise risk. Checked as of 2026-05-21; role: curriculum_anchor.
[of Standards and Technology, 2022b]	Systems-security engineering foundation for trustworthy systems in contested operational environments and related training programs. Checked as of 2026-05-21; role: curriculum_anchor.
[of Standards and Technology, 2024b]	Official NIST operational technology security guidance. Checked as of 2026-05-21; role: source_quality_anchor.
[of Automation, 2026]	Official ISA overview of industrial automation and control security standards. Checked as of 2026-05-21; role: source_quality_anchor.
[Cybersecurity and Agency, 2026a]	Official prioritized baseline of IT and OT cybersecurity practices for critical-infrastructure risk reduction and maturity assessment. Checked as of 2026-05-21; role: curriculum_anchor.
[Cybersecurity and Agency, 2026c]	Official defensive ICS practice library for defense-in-depth, forensics, incident response, and remote access. Checked as of 2026-05-21; role: curriculum_anchor.
[MITRE, 2026c]	Threat-informed defensive matrix for ICS tactics and techniques, used for coverage mapping. Checked as of 2026-05-21; role: curriculum_anchor.

66.3.5.1 Threat Intelligence Sharing for Critical Infrastructure evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [253, 2026]; [258, 2026].

66.3.6 Threat Intelligence Sharing for Critical Infrastructure agentic boundary: assist, approve, block, and record

Evidence anchor. Section 66; [253, 2026].

AGEINT translation is bounded by the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC**.

66.3.6.1 Threat Intelligence Sharing for Critical Infrastructure permitted defensive utility: curriculum uses and safe outputs

Evidence anchor. Section 66; [253, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC**.

66.3.6.2 Threat Intelligence Sharing for Critical Infrastructure excluded operational boundary: blocked actions and stop rules

Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [253, 2026]; [258, 2026] and **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

66.3.7 Threat Intelligence Sharing for Critical Infrastructure governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 66; [253, 2026].

Governance is practiced as a gate on the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane. Learners use the **Cyber-Physical Readiness Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC**.

66.3.7.1 Threat Intelligence Sharing for Critical Infrastructure governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [253, 2026]; [258, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **ICS/OT Cyber-Physical Defense and Tabletop Readiness** failure modes and the **Cyber-Physical Readiness Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

66.3.7.2 Threat Intelligence Sharing for Critical Infrastructure evidence package handoff: appendices, records, and reuse Evidence anchor.

Section 66; [253, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Cyber-Physical Readiness Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC**.

66.3.7.3 Threat Intelligence Sharing for Critical Infrastructure current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC**. [253, 2026]; [258, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_nist_csf_2` for **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC**?	The NIST Cybersecurity Framework (CSF) 2.0; lane `ics_ot_defense`; checked 2026-05-21.	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric; Official cybersecurity-risk governance framework that adds the Govern function and supplies a common language for AI, OT, and enterprise risk.
What does the module inherit from `official_nist_sp_800_160r1` for **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC**?	Engineering Trustworthy Secure Systems, NIST SP 800-160 Vol. 1 Rev. 1; lane `ics_ot_defense`; checked 2026-05-21.	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric; Systems-security engineering foundation for trustworthy systems in contested operational environments and related training programs.
What does the module inherit from `official_nist_sp_800_82r3` for **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC**?	Guide to Operational Technology Security, NIST SP 800-82 Rev. 3; lane `source_quality_spine`; checked 2026-05-21.	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric; Official NIST operational technology security guidance.
What does the module inherit from `official_isa_iec_62443` for **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC**?	ISA/IEC 62443 Series of Standards; lane `source_quality_spine`; checked 2026-05-21.	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric; Official ISA overview of industrial automation and control security standards.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 66; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

66.3.8 Threat Intelligence Sharing for Critical Infrastructure assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 66; [253, 2026].

66.3.9 Threat Intelligence Sharing for Critical Infrastructure assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 66; [253, 2026].

66.3.9.1 Threat Intelligence Sharing for Critical Infrastructure capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC** and [253, 2026]; [258, 2026].

66.3.9.2 Threat Intelligence Sharing for Critical Infrastructure instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC** and [253, 2026]; [258, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

66.3.9.3 Threat Intelligence Sharing for Critical Infrastructure assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Evidence-Driven Analysis of Threat Information Sharing for ICS (arXiv 2025)	Completed **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
ISACs: E-ISAC, WaterISAC, FS-ISAC	Completed **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
CISA Frameworks for Critical Infrastructure	Completed **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

66.3.10 Threat Intelligence Sharing for Critical Infrastructure refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [253, 2026]; [258, 2026] and **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC**.

66.3.10.1 Threat Intelligence Sharing for Critical Infrastructure refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC**. The local signals begin with [253, 2026]; [258, 2026].

66.3.10.2 Threat Intelligence Sharing for Critical Infrastructure claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC**, and the source spine for these checks begins with [253, 2026]; [258, 2026].

66.3.11 Threat Intelligence Sharing for Critical Infrastructure reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [253, 2026]; [258, 2026].

Triangulation anchors. In module 48's review-checklist section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC**. [253, 2026]; [258, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.

- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

66.3.12 Threat Intelligence Sharing for Critical Infrastructure learning-path links: module map, overview, and curriculum atlas

Use the cross-links below to place **Evidence-Driven Analysis of Threat Information Sharing for ICS; ISACs: E-ISAC, WaterISAC, FS-ISAC** in the wider unit: the orientation sets the frame, the parent unit supplies the shared safety posture, and the neighbouring modules show what evidence enters and leaves. Lead sources: [253, 2026]; [258, 2026].

Section 2, Section 62, Section 65, Section 67

67 AGEINT Applied to ICS and Cyber-Physical Intelligence

67.0.1 AGEINT Applied to ICS and Cyber-Physical Intelligence figures and course links: visual evidence, source flow, and navigation

The module uses Figure 141, Figure 142, and Figure 134 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.

Navigation links: Section 2, Section 62, Section 66, Section 68.

This module teaches the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane through a bounded, source-backed coursebook chapter. [255, 2026]; [256, 2026].

67.1 ICS/OT Cyber-Physical Defense and Tabletop Readiness frame for AGEINT Applied to ICS and Cyber-Physical Intelligence: source context, topic focus, and reader task

Evidence anchor. Section 67; [255, 2026].

67.1.1 AGEINT Applied to ICS and Cyber-Physical Intelligence orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 67; [255, 2026].

67.1.2 AGEINT Applied to ICS and Cyber-Physical Intelligence conceptual primer: source context, core model, and reader task

This chapter teaches ICS/OT intelligence as safety-aware defensive reasoning: asset state, engineering consequence, operator decision, and recovery evidence matter as much as cyber indicators. The chapter uses **Cyber-Physical Readiness Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**.

The central distinction is to separate cyber analysis from unsafe process control or live operational action. Core topics include **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation; ICS defensive coverage and safety tabletop using synthetic process records**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.

Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [255, 2026]; [256, 2026].

Learners move from vocabulary and the **Cyber-Physical Readiness Lens** distinction through topic lessons on **AI-Driven Anomaly Detection in OT Networks** with evidence and misconception checks, then assemble a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** with safety and rights gates.

67.1.3 AGEINT Applied to ICS and Cyber-Physical Intelligence learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 67; [255, 2026].

- Connect **AI-Driven Anomaly Detection in OT Networks and LLM Agents for ICS Log Analysis and Threat Correlation** to **ICS/OT Cyber-Physical Defense and Tabletop Readiness** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate cyber analysis from unsafe process control or live operational action; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as IT-first assumptions, unsafe automation, untested shutdown logic, poor remote-access control, and missing after-action learning, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: all ICS work remains tabletop, lab, or accountable defensive review; no exploitation, unsafe process manipulation, or live control actions.

67.1.4 AGEINT Applied to ICS and Cyber-Physical Intelligence core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 67; [255, 2026].

Term	Working definition
Engineering state	the physical or process condition that gives cyber evidence safety meaning
Consequence	the operational, safety, environmental, or service effect of a condition
Defense in depth	layered prevention, detection, response, and recovery controls
Tabletop inject	a synthetic event used to rehearse decisions without touching live systems
Recovery evidence	proof that a safe state, service, or learning objective was restored
AI-Driven Anomaly Detection in OT Networks	Key terms: AI, Driven, Anomaly.
LLM Agents for ICS Log Analysis and Threat…	Key terms: LLM, Agents, ICS.

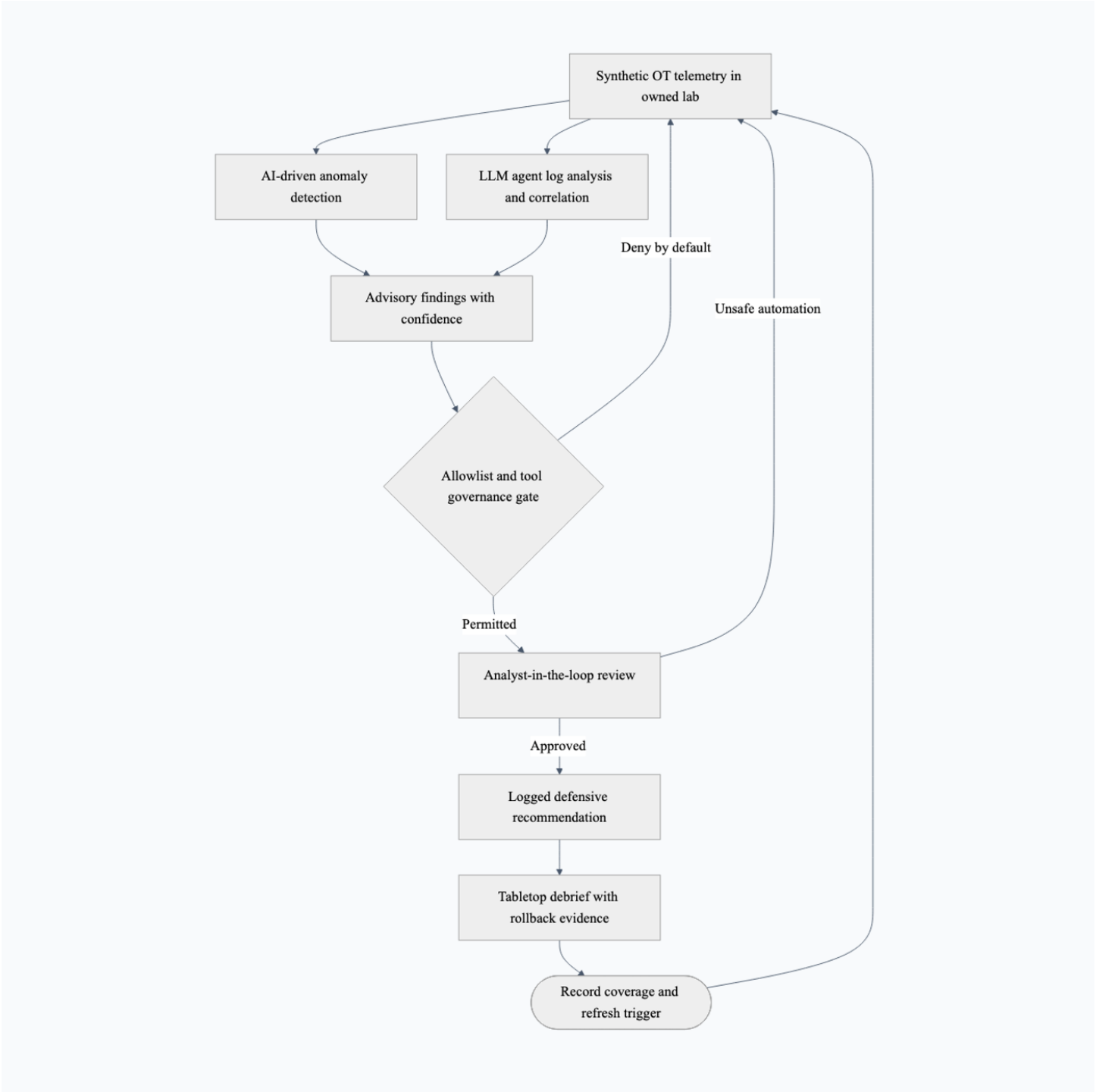


Figure 141: A bounded assurance loop for AI-assisted ICS defense where anomaly findings stay advisory and every action runs in an owned lab with logging and rollback. The captioned view belongs to the industrial and cyber physical intelligence / ageint applied to ics and cyber physical intelligence section and should be read as a map of Synthetic OT telemetry in owned lab, AI-driven anomaly detection, LLM agent log analysis and correlation, and Advisory findings with confidence, not as a capability score or live-task instruction.

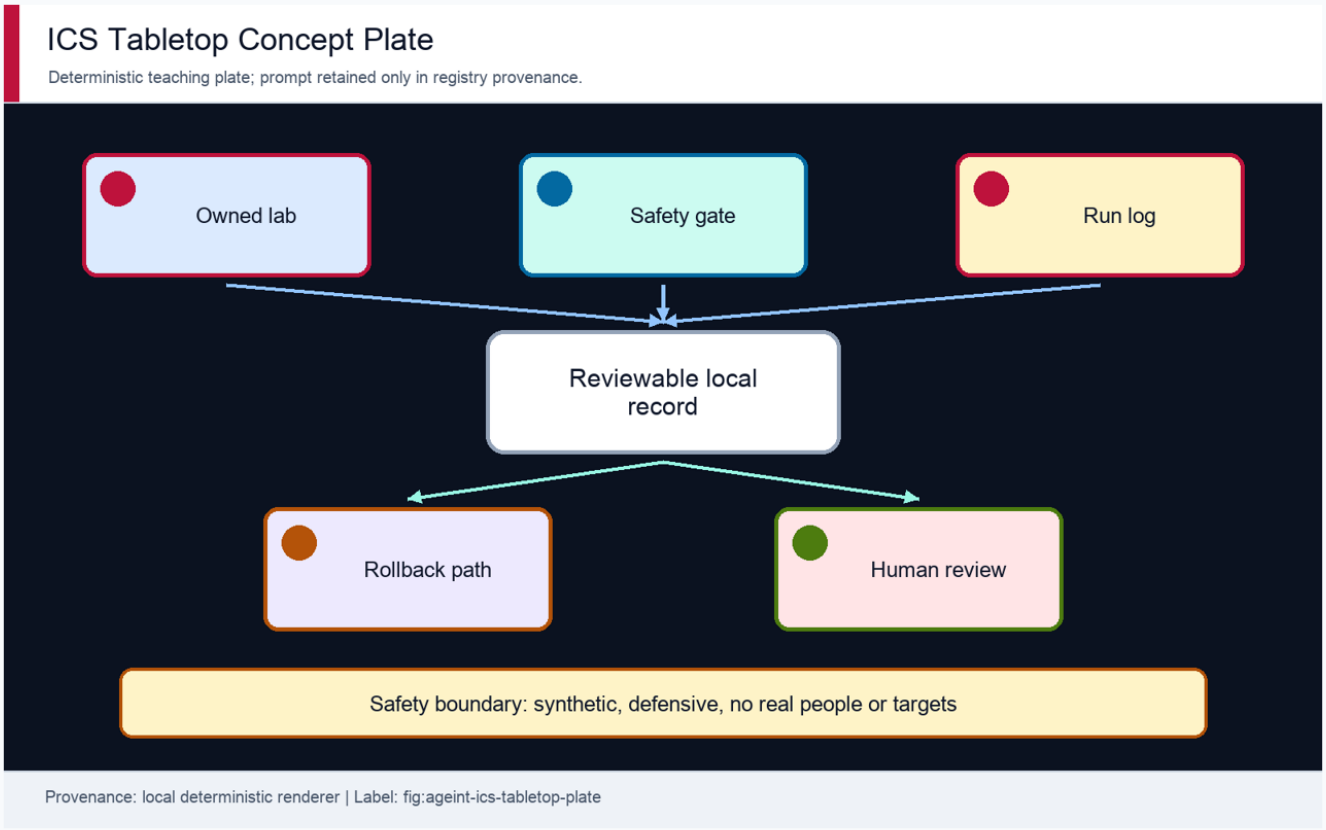


Figure 142: Deterministic teaching plate for ICS tabletop learning with owned-lab fixtures, logging, rollback, and defensive review. The captioned view belongs to the industrial and cyber physical intelligence / ageint applied to ics and cyber physical intelligence section and should be read as a map of Owned lab, Safety gate, Run log, and Rollback path, not as a capability score or live-task instruction.

67.2 Cyber-Physical Readiness Lens path for AGEINT Applied to ICS and Cyber-Physical Intelligence: lesson cluster, safe artifact, and review

Evidence anchor. Section 67; [255, 2026].

67.2.1 AGEINT Applied to ICS and Cyber-Physical Intelligence practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 67; [255, 2026].

67.2.2 AGEINT Applied to ICS and Cyber-Physical Intelligence topic lessons: source-backed concepts and transfer tasks

This module builds ICS/OT intelligence as safety-aware defensive reasoning: asset state, engineering consequence, operator decision, and recovery evidence matter as much as cyber indicators. The sequence opens with **AI-Driven Anomaly Detection in OT Networks**, **LLM Agents for ICS Log Analysis and Threat Correlation**, **ICS defensive coverage and safety tabletop using synthetic process records** and applies the **Cyber-Physical Readiness Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 134; module overview Section 67; curriculum atlas Section 2.

Triangulation anchors. In module 49's topic-lessons section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

67.2.2.1 Lesson 1: AI-Driven Anomaly Detection in OT Networks **Concept. AI-Driven Anomaly Detection in OT Networks** applies AI, Driven, Anomaly within ICS/OT Cyber-Physical Defense and Tabletop Readiness: learners use separate cyber analysis from unsafe process control or live operational action and safety-aware tabletop readiness and defensive coverage review evidence before any judgment moves forward.

Why it matters. AI-Driven Anomaly Detection matters in the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane because safety-aware tabletop readiness and defensive coverage evidence must stay separate from judgment; IT-first assumptions is a common failure.

Source support. AI-Driven Anomaly Detection in OT Networks rests on [307, 2026], [305, 2026], and [304, 2026]. The most specific cited work observes: NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Use them for the claim that **AI-Driven Anomaly Detection in OT Networks** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. Read **AI-Driven Anomaly Detection** against the works cited for this row. [307, 2026] Official CISA Industrial Control Systems recommended practices page for defensive ICS/OT safety, resilience, and incident-preparation guidance. [305, 2026] Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **AI-Driven Anomaly Detection**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must name the source descriptor, the bounded claim about **AI-Driven Anomaly Detection in OT**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **AI-Driven Anomaly Detection** work as a **cyber-physical tabletop evidence packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that AI-Driven Anomaly Detection in OT Networks replaces human review whenever evidence looks plausible.

Transfer task. Transfer **AI-Driven Anomaly Detection** to a second module by preserving safety-aware tabletop readiness and defensive coverage review, changing the source evidence, and naming a new reviewer.

67.2.2.2 Lesson 2: LLM Agents for ICS Log Analysis and Threat Correlation **Concept. LLM Agents for ICS Log Analysis and Threat Correlation** treats agents as software actors with explicit permissions, logs, stop conditions, and human approval—not autonomous decision makers.

Why it matters. LLM Agents for ICS Log Analysis and Threat Correlation connects classroom vocabulary to ICS/OT Cyber-Physical Defense and Tabletop Readiness practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. LLM Agents for ICS Log Analysis and Threat Correlation rests on [299, 2026], [306, 2026], and [312, 2026]. The closest source to this row notes: It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). Use them for pinning down the scope of **LLM Agents for ICS Log Analysis and Threat Correlation**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. For **LLM Agents for ICS Log Analysis and Threat Correlation**, reason from the sources cited in this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **LLM Agents for ICS Log Analysis and Threat Correlation**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must name the source descriptor, the bounded claim about **LLM Agents for ICS Log**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape this subject work as a **cyber-physical tabletop evidence packet** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception that LLM Agents for ICS Log Analysis and Threat Correlation can be used while ignoring the rule to separate cyber analysis from unsafe process control or live operational action.

Transfer task. Transfer **LLM Agents for ICS Log Analysis and Threat Correlation** to a second module by preserving safety-aware tabletop readiness and defensive coverage review, changing the source evidence, and naming a new reviewer.

67.2.2.3 Lesson 3: ICS defensive coverage and safety tabletop using synthetic process records **Concept. ICS defensive coverage and safety tabletop using synthetic process records** maps incident phases to evidence preservation, stakeholder notification, learning loops, and

defensive control updates.

Why it matters. Without explicit treatment of **ICS defensive coverage**, IT-first assumptions undermines safety-aware tabletop readiness and defensive coverage review; the lesson builds the habit to separate cyber analysis from unsafe process control or live operational action.

Source support. ICS defensive coverage and safety tabletop using synthetic process records rests on [213, 2026]. The most specific cited work observes: The matrix organizes methods into twelve tactical categories spanning initial access through impact, including ICS-specific concerns such as firmware modification and disruption of operational technology. Use it for the claim that **ICS defensive coverage and safety tabletop using synthetic process records** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. For **ICS defensive coverage**, reason from the sources cited in this row. [213, 2026] The Industrial Control Systems (ICS) domain of the MITRE ATT&CK framework, a knowledge base documenting adversary behaviors based on real-world observations of attacks on critical infrastructure. The matrix organizes methods into twelve tactical categories spanning initial access through impact, including ICS-specific concerns such as firmware modification and disruption of operational technology. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **ICS defensive coverage**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must list the asset descriptor, the bounded claim about **ICS defensive coverage and safety**, the safety caveat, the uncertainty note, the no-live-actuation boundary, and the reviewer who owns the safety case. Shape **ICS defensive coverage** work as a **cyber-physical tabletop evidence packet** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **ICS defensive coverage**: that an industrial control system behaving normally proves it is safe, rather than a state that depends on intact safeguards and monitoring.

Transfer task. Apply this module's safe boundary for **ICS defensive coverage** to another artifact while keeping safety-aware tabletop readiness and defensive coverage review and reviewer ownership explicit.

67.2.2.4 Lesson 4: AGEINT for SCADA Data Fusion and Pattern-of-Process Analysis

Concept. AGEINT for SCADA Data Fusion and Pattern-of-Process Analysis maps industrial assets, safety interlocks, operator roles, and consequence before any cyber-physical inference.

Why it matters. Analysts use **AGEINT for SCADA Data Fusion and Pattern-of-Process Analysis** to separate cyber analysis from unsafe process control or live operational action. A defensible treatment names the judgment it enables for safety-aware tabletop readiness and defensive coverage review, the proof limit that IT-first assumptions would otherwise hide, and the reviewer accountable for challenge.

Source support. AGEINT for SCADA Data Fusion and Pattern-of-Process Analysis rests on [307, 2026], [305, 2026], and [304, 2026]. The most specific cited work observes: NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Use them for pinning down the scope of **AGEINT for SCADA Data Fusion and Pattern-of-Process Analysis**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. Read **AGEINT for SCADA Data Fusion and Pattern-of-Process Analysis** against the works cited for this row. [307, 2026] Official CISA Industrial Control Systems recommended practices page for defensive ICS/OT safety, resilience, and incident-preparation guidance. [305, 2026] Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **AGEINT for SCADA Data Fusion and Pattern-of-Process Analysis**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must name the source descriptor, the bounded claim about **AGEINT for SCADA Data Fusion**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape this subject work as a **cyber-physical tabletop evidence packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that AGEINT for SCADA Data Fusion and Pattern-of-Process Analysis establishes intent without reviewing alternative explanations.

Transfer task. Transfer **AGEINT for SCADA Data Fusion and Pattern-of-Process Analysis** to a second module by preserving safety-aware tabletop readiness and defensive coverage review, changing the source evidence, and naming a new reviewer.

67.2.2.5 Lesson 5: Digital Twins for Industrial Intelligence: Simulation and Red Team

Concept. Digital Twins for Industrial Intelligence: Simulation and Red Team structures evaluation as misuse-case testing with blocked outcomes, logged evidence, and reviewer disposition.

Why it matters. Digital Twins for Industrial Intelligence matters in the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane because safety-aware tabletop readiness and defensive coverage evidence must stay separate from judgment; IT-first assumptions is a common failure.

Source support. Digital Twins for Industrial Intelligence: Simulation and Red Team rests on [300, 2026], [304, 2026], and [306, 2026]. The most specific cited work observes: NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. Use them for fixing what **Digital Twins for Industrial Intelligence: Simulation and Red Team** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. For **Digital Twins for Industrial Intelligence**, work from the cited evidence behind this row. [300, 2026] MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy. [304, 2026] NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences. [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **Digital Twins for Industrial Intelligence**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must name the source descriptor, the bounded claim about **Digital Twins for Industrial Intelligence**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Digital Twins for Industrial Intelligence** work as a **cyber-physical tabletop evidence packet** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception that Digital Twins for Industrial Intelligence: Simulation and Red Team replaces human review whenever evidence looks plausible.

Transfer task. Transfer **Digital Twins for Industrial Intelligence** to a second module by preserving safety-aware tabletop readiness and defensive coverage review, changing the source evidence, and naming a new reviewer.

67.2.2.6 Lesson 6: Multi-Agent Systems for Critical Infrastructure Protection

Concept. Multi-Agent Systems for Critical Infrastructure Protection evaluates ISAC sharing by handling rules, anonymization, confidence, and consumer responsibilities.

Why it matters. Analysts use **Multi-Agent Systems** to separate cyber analysis from unsafe process control or live operational action. A defensible treatment names the judgment it enables for safety-aware tabletop readiness and defensive coverage review, the proof limit that IT-first assumptions would otherwise hide, and the reviewer accountable for challenge.

Source support. Multi-Agent Systems for Critical Infrastructure Protection rests on [299, 2026], [306, 2026], and [312, 2026]. Its anchor reference records: It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). Use them for fixing what **Multi-Agent Systems for Critical Infrastructure Protection** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b].

Evidence to inspect. For **Multi-Agent Systems**, work from the cited evidence behind this row. [299, 2026] The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation). [306, 2026] Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support. [312, 2026] Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Multi-Agent Systems**, build a **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** for this safety-aware tabletop readiness and defensive coverage review topic. The artifact must name the source descriptor, the bounded claim about **Multi-Agent Systems for Critical Infrastructure**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Multi-Agent Systems** work as a **cyber-physical tabletop evidence packet** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that Multi-Agent Systems for Critical Infrastructure Protection can be used while ignoring the rule to separate cyber analysis from unsafe process control or live operational action.

Transfer task. Transfer **Multi-Agent Systems** to a second module by preserving safety-aware tabletop readiness and defensive coverage review, changing the source evidence, and naming a new reviewer.

67.2.3 AGEINT Applied to ICS and Cyber-Physical Intelligence worked safe example: synthetic inputs, evidence, and review

Worked example: a sample water-utility tabletop reviews synthetic process logs after a simulated anomaly. [255, 2026]; [256, 2026].

Triangulation anchors. In module 49's worked-example section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **safety-aware ICS and OT intelligence**. Learners use a **cyber-physical tabletop evidence packet** and keep this boundary visible: No live device control, unsafe process change, exploit sequence, evasion, or operational response.

Frame. The classroom question centers on **AI-Driven Anomaly Detection in OT Networks**. Excluded actions stay explicit, and the **Cyber-Physical Readiness Lens** planning question is: Which asset, architecture record, consequence, operator decision, and recovery path is being exercised defensively?

Inputs. For the **AI-Driven Anomaly Detection in OT Networks** scenario, use toy HMI screenshots, fabricated network alerts, public ICS control guidance, and a safety stop card. The Cyber-Physical Readiness Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **AI-Driven Anomaly Detection in OT Networks**, students map assets to consequences, classify tabletop injects, identify human decisions, and preserve recovery evidence. Pause whenever an inference about AI-Driven Anomaly Detection in OT Networks appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **AI-Driven Anomaly Detection in OT Networks** classroom scenario; unit artifact = cyber-physical tabletop evidence packet; evidence = allowed inputs; method = safety-aware tabletop readiness and defensive coverage review; output = a cyber-physical tabletop packet with assets, consequences, ATT&CK mapping, decisions, and debrief; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **AI-Driven Anomaly Detection in OT Networks** as "Cyber-Physical Readiness Lens confirms it" is not enough. The revision ties the claim to safety-aware tabletop readiness and defensive coverage review, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **AI-Driven Anomaly Detection in OT Networks** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

67.2.4 AGEINT Applied to ICS and Cyber-Physical Intelligence practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Cyber-Physical Readiness Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**.

Triangulation anchors. In module 49's practice-sequence section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare AI-Driven Anomaly Detection in OT Networks, LLM Agents for ICS Log Analysis and Threat Correlation, ICS defensive coverage and safety tabletop using synthetic process records; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane.

Move	Learner action	Output	Check
2. Frame	Answer the lens question: Which asset, architecture record, consequence, operator decision, and recovery path is being exercised defensively?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for AI-Driven Anomaly Detection in OT Networks: tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the cyber-physical tabletop evidence packet fields for AI-Driven Anomaly Detection in OT Networks.	Unit profile note.	Evidence artifacts include asset-consequence map, operator decision log.
4. Challenge	Test the misconception that AI-Driven Anomaly Detection in OT Networks replaces human review whenever evidence looks plausible.	Failure-mode note.	The artifact applies the key distinction: separate cyber analysis from unsafe process control or live operational action.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

67.2.4.1 AGEINT Applied to ICS and Cyber-Physical Intelligence instructor notes: source reasoning, review points, and studio focus Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**. [255, 2026]; [256, 2026].

67.2.4.2 AGEINT Applied to ICS and Cyber-Physical Intelligence extension exercise: peer validation and refresh trigger review
Evidence anchor. Section 67; [255, 2026].
Have learners swap artifacts and apply the **Cyber-Physical Readiness Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**.

67.2.5 AGEINT Applied to ICS and Cyber-Physical Intelligence knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 67; [255, 2026].

1. Explain how **AI-Driven Anomaly Detection in OT Networks** is defined here; name the source descriptor that supports the definition.
2. Contrast **AI-Driven Anomaly Detection in OT Networks** with **LLM Agents for ICS Log Analysis and Threat Correlation** using the **Cyber-Physical Readiness Lens** artifact fields.
3. Identify one failure mode from the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane and the evidence that would reveal it.
4. Answer the coursebook review question: Which cyber observation changes meaning once physical consequence is considered?
5. Correct this misconception: that AI-Driven Anomaly Detection in OT Networks replaces human review whenever evidence looks plausible.

67.2.5.1 AGEINT Applied to ICS and Cyber-Physical Intelligence answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **AI-Driven Anomaly Detection in OT Networks** without source evidence, uncertainty, or a safe transfer task.

67.3 AGEINT Applied to ICS and Cyber-Physical Intelligence assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 67; [255, 2026].

67.3.1 AGEINT Applied to ICS and Cyber-Physical Intelligence evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 67; [255, 2026].

67.3.2 AGEINT Applied to ICS and Cyber-Physical Intelligence transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 67; [255, 2026].

67.3.2.1 AGEINT Applied to ICS and Cyber-Physical Intelligence lineage and source tradition: profile, concepts, and first anchors

This sits in the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lineage: defensive intelligence for safety-critical environments where availability, engineering state, and physical consequence matter. [255, 2026]; [256, 2026].

67.3.2.2 AGEINT Applied to ICS and Cyber-Physical Intelligence working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 67; [255, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**, with provenance and reviewability throughout.

67.3.2.3 AGEINT Applied to ICS and Cyber-Physical Intelligence knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** synthetic process logs, asset/consequence maps, operator decisions, safety stops, and recovery evidence. [255, 2026]; [256, 2026].
- **Transforms:** asset-consequence mapping, ATT&CK-for-ICS coverage review, operator-decision rehearsal, and after-action learning.
- **Outputs:** cyber-physical tabletop packet, debrief rubric, recovery note, and control-coverage map.
- **Failure modes:** IT-first assumptions, unsafe actuation, live-control drift, and missing safety review.

67.3.2.4 AGEINT Applied to ICS and Cyber-Physical Intelligence transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 67; [255, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**.
- **Evidence contract:** keep the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as cyber-physical tabletop packet, debrief rubric, recovery note, and control-coverage map that another reviewer can audit.

67.3.2.5 AGEINT Applied to ICS and Cyber-Physical Intelligence profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 67; [255, 2026].

The matched profile emphasizes defensive intelligence for safety-critical environments where availability, engineering state, and physical consequence matter. The method stack is asset/consequence mapping, ATT&CK-for-ICS coverage review, defense-in-depth audit, remote-access check, and tabletop injects; the local topic cluster is **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**.

67.3.3 AGEINT Applied to ICS and Cyber-Physical Intelligence evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 67; [255, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** profile tells reviewers what evidence is strong enough for the module artifact built around **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**.

67.3.3.1 AGEINT Applied to ICS and Cyber-Physical Intelligence guide source spine: inherited keys and local citation roles

Primary guide citations: [255, 2026]; [256, 2026]; [257, 2026]; [273, 2026]; [274, 2026]; [275, 2026]; [286, 2026]; [287, 2026]; [292, 2026]; [213, 2026]; [307, 2026]; [305, 2026]; [304, 2026]; [299, 2026]; [306, 2026]; [312, 2026]; [300, 2026].

67.3.3.2 AGEINT Applied to ICS and Cyber-Physical Intelligence verified source canon: direct anchors and claim boundaries

The source canon has three tiers; the local spine begins with [255, 2026]; [256, 2026].

Tier	What counts	How it is used
Source guide	[255, 2026]; [256, 2026]; [257, 2026]; [273, 2026]; [274, 2026]; [275, 2026]; [286, 2026]; [287, 2026]; [292, 2026]; [213, 2026]; [307, 2026]; [305, 2026]; [304, 2026]; [299, 2026]; [306, 2026]; [312, 2026]; [300, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 49's source-canon section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation** and [255, 2026]; [256, 2026], but only directly verified source URLs are encoded as citations.

67.3.3.3 AGEINT Applied to ICS and Cyber-Physical Intelligence intelligence practice lens: evidence artifact and safety check

Practice lens: **Cyber-Physical Readiness Lens** for **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**. [255, 2026]; [256, 2026].

Planning question: Which asset, architecture record, consequence, operator decision, and recovery path is being exercised defensively?

Evidence artifact: tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric.

Validation rule: validate against safety, availability, engineering state, incident scope, and after-action learning. Applied to **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**.

Handoff contract: separate cyber indicators, process observations, safety impact, operator choices, and recovery evidence.

Safety check: keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions.

67.3.3.4 AGEINT Applied to ICS and Cyber-Physical Intelligence runtime-to-reader map: generated sections and verifier surfaces

Evidence anchor. Section 67; [255, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	49.99	49.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind AGEINT Applied to ICS and Cyber-Physical Intelligence to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Bounded autonomy, procurement, incident-response, and assurance studio	49.101	49.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for AGEINT Applied to ICS and Cyber-Physical Intelligence	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Model-card, recoverability, retention, and learner-support evidence package	49.102	49.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for AGEINT Applied to ICS and Cyber-Physical Intelligence	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
AI-Driven Anomaly Detection in OT Networks	49.1	49.1 AI-Driven Anomaly Detection in OT Networks	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
LLM Agents for ICS Log Analysis and Threat Correlation	49.2	49.2 LLM Agents for ICS Log Analysis and Threat Correlation	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
ICS defensive coverage and safety tabletop using synthetic process records	49.3	49.3 source title transformed into safe curriculum treatment; original: Autonomous ICS Incident Response: AGEINT Pattern 16 in OT	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
AGEINT for SCADA Data Fusion and Pattern-of-Process Analysis	49.4	49.4 AGEINT for SCADA Data Fusion and Pattern-of-Process Analysis	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Digital Twins for Industrial Intelligence: Simulation and Red Team	49.5	49.5 Digital Twins for Industrial Intelligence: Simulation and Red Team	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Multi-Agent Systems for Critical Infrastructure Protection	49.6	49.6 Multi-Agent Systems for Critical Infrastructure Protection	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions

67.3.3.5 AGEINT Applied to ICS and Cyber-Physical Intelligence reusable subsection contract: topic rows, artifacts, and safety duties Evidence anchor. Section 67; [255, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
AI-Driven Anomaly Detection in OT Networks	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
LLM Agents for ICS Log Analysis and Threat Correlation	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
ICS defensive coverage and safety tabletop using synthetic process records	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
AGEINT for SCADA Data Fusion and Pattern-of-Process Analysis	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Digital Twins for Industrial Intelligence: Simulation and Red Team	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions
Multi-Agent Systems for Critical Infrastructure Protection	Cyber-Physical Readiness Lens	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric	keep exercises lab-only or tabletop; exclude exploitation, process manipulation, unsafe actuation, and live-control actions

67.3.3.6 AGEINT Applied to ICS and Cyber-Physical Intelligence annotated source ledger: real titles and local contribution Each source cited by this **ICS/OT Cyber-Physical Defense and Tabletop Readiness** module is paired below with its real title and a one-line note on what it contributes to **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**.

Source	Cited work	What it contributes	Status
[255, 2026]	Web of Things (WoT) Architecture 1.1	The W3C Recommendation for Web of Things Architecture 1.1, published in December 2023, defining an abstract architecture for interoperability across diverse Internet of Things platforms. It introduces core concepts including Things described by machine-readable Thing Descriptions, reusable Thing Models, and Consumers that interpret descriptions to interact via Properties, Actions, and Events.	verified source-guide
[256, 2026]	Web of Things (WoT) Thing Description 1.1	The W3C WoT Thing Description 1.1 is a formal information model and standardized representation format enabling IoT devices to describe their metadata and interaction capabilities in a machine-readable way, facilitating interoperability across diverse ecosystems.	verified source-guide
[257, 2026]	Web of Things (WoT) Discovery	A W3C Recommendation for Web of Things (WoT) Discovery, published December 5, 2023 by the W3C Web of Things Working Group. It specifies how IoT devices and services can be discovered and how their Thing Description metadata can be accessed securely, using a two-phase model of Introduction and Exploration.	verified source-guide
[273, 2026]	WCAG 2 Overview	The W3C Web Accessibility Initiative overview of the Web Content Accessibility Guidelines (WCAG), an international standard for making web content accessible to people with disabilities. It explains that WCAG is organized around four principles (perceivable, operable, understandable, robust) with testable success criteria at three conformance levels (A, AA, AAA), and covers versions 2.0, 2.1, and 2.2.	verified source-guide
[274, 2026]	CAST Universal Design for Learning Guidelines version 3.0	The official CAST website for the Universal Design for Learning (UDL) Guidelines version 3.0, released in 2024. The framework offers research-based guidance for designing inclusive learning environments and is organized around three principles: Engagement (motivation and emotional support), Representation (accessible presentation of information), and Action and Expression (diverse means of participation and communication).	verified source-guide
[275, 2026]	Fact Sheet: New Rule on the Accessibility of Web Content and Mobile Apps Provided by State and Local Governments	A US Department of Justice fact sheet explaining the 2024 ADA Title II rule requiring state and local governments to make their web content and mobile apps accessible. It establishes WCAG 2.1 Level AA as the technical standard, applies to entities such as schools, courts, libraries, and transit agencies, and sets compliance deadlines of April 2027 for larger jurisdictions and April 2028 for smaller ones.	verified source-guide

Source	Cited work	What it contributes	Status
[286, 2026]	Model Cards for Model Reporting	The arXiv abstract for "Model Cards for Model Reporting" (2018) by Mitchell, Wu, Zaldivar, and colleagues, which introduces a framework for transparent documentation of machine learning models. Model cards are short accompanying documents that report a model's benchmarked performance across varied conditions, including different cultural, demographic, and phenotypic groups, along with intended use, evaluation methodology, and deployment considerations.	verified source-guide
[287, 2026]	Datasheets for Datasets	A 2018 arXiv paper proposing 'datasheets for datasets,' a standardized documentation framework for machine learning datasets modeled on electronic component datasheets. The authors argue the field lacks consistent dataset documentation, which creates risk in high-stakes applications, and propose that datasets be accompanied by documentation covering motivation, composition, collection process, recommended uses, and test results.	verified source-guide
[292, 2026]	Assessing Risks and Impacts of AI (ARIA): Pilot Evaluation Report	The ARIA 0.1 pilot evaluation report documents NIST's methodology for systematically assessing AI applications for risks and societal impacts, using a multi-layered evaluation approach across five participating organizations and seven submitted AI applications. The pilot employed three evaluation scenarios and three testing levels: model testing, red teaming, and field testing, supplemented by dialogue annotation, tester questionnaires, and structured measurement trees.	verified source-guide
[213, 2026]	ICS Matrix - MITRE ATT&CK®	The Industrial Control Systems (ICS) domain of the MITRE ATT&CK framework, a knowledge base documenting adversary behaviors based on real-world observations of attacks on critical infrastructure. The matrix organizes methods into twelve tactical categories spanning initial access through impact, including ICS-specific concerns such as firmware modification and disruption of operational technology.	verified source-guide
[307, 2026]	ICS Recommended Practices	Official CISA Industrial Control Systems recommended practices page for defensive ICS/OT safety, resilience, and incident-preparation guidance.	original source-guide
[305, 2026]	DevSecOps	Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support.	original source-guide

Source	Cited work	What it contributes	Status
[304, 2026]	Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities	NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences.	verified source-guide
[299, 2026]	Model Context Protocol Specification	The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation).	verified source-guide context; use pinned MCP anchor for normative claims
[306, 2026]	Artificial Intelligence	Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support.	original source-guide
[312, 2026]	Guide on the Use of Agentic Artificial Intelligence	Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support.	original source-guide
[300, 2026]	MITRE ATLAS	MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy.	original source-guide

Where this sits. This module's overview is Section 67; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

67.3.4 AGEINT Applied to ICS and Cyber-Physical Intelligence governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 67; [255, 2026].

67.3.5 AGEINT Applied to ICS and Cyber-Physical Intelligence analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 49's governance-boundary section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **ICS/OT Cyber-Physical Defense and Tabletop Readiness** for **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**. [255, 2026]; [256, 2026].

Curriculum topic spine: AI-Driven Anomaly Detection in OT Networks, **LLM Agents for ICS Log Analysis and Threat Correlation**, **ICS defensive coverage and safety tabletop using synthetic process records**. **Verified anchor cluster:** [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]; [Cybersecurity and Agency, 2026a]; [Cybersecurity and Agency, 2026c]; [MITRE, 2026c].

Conceptual depth: defensive intelligence for safety-critical environments where availability, engineering state, and physical consequence matter.

Method stack: asset/consequence mapping, ATT&CK-for-ICS coverage review, defense-in-depth audit, remote-access check, and tabletop injects.

Composability contract: separate cyber indicators, engineering observations, safety impacts, operator decisions, and recovery actions.

Known failure modes: IT-first assumptions, unsafe automation, untested shutdown logic, poor remote-access control, and missing after-action learning.

Defensive boundary: all ICS work remains tabletop, lab, or accountable defensive review; no exploitation, unsafe process manipulation, or live control actions. Applied to **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**.

Anchor	Why it matters here
[of Standards and Technology, 2024f]	Official cybersecurity-risk governance framework that adds the Govern function and supplies a common language for AI, OT, and enterprise risk. Checked as of 2026-05-21; role: curriculum_anchor.
[of Standards and Technology, 2022b]	Systems-security engineering foundation for trustworthy systems in contested operational environments and related training programs. Checked as of 2026-05-21; role: curriculum_anchor.
[of Standards and Technology, 2024b]	Official NIST operational technology security guidance. Checked as of 2026-05-21; role: source_quality_anchor.
[of Automation, 2026]	Official ISA overview of industrial automation and control security standards. Checked as of 2026-05-21; role: source_quality_anchor.
[Cybersecurity and Agency, 2026a]	Official prioritized baseline of IT and OT cybersecurity practices for critical-infrastructure risk reduction and maturity assessment. Checked as of 2026-05-21; role: curriculum_anchor.
[Cybersecurity and Agency, 2026c]	Official defensive ICS practice library for defense-in-depth, forensics, incident response, and remote access. Checked as of 2026-05-21; role: curriculum_anchor.
[MITRE, 2026c]	Threat-informed defensive matrix for ICS tactics and techniques, used for coverage mapping. Checked as of 2026-05-21; role: curriculum_anchor.

67.3.5.1 AGEINT Applied to ICS and Cyber-Physical Intelligence evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [255, 2026]; [256, 2026].

67.3.6 AGEINT Applied to ICS and Cyber-Physical Intelligence agentic boundary: assist, approve, block, and record

Evidence anchor. Section 67; [255, 2026].

AGEINT translation is bounded by the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**.

67.3.6.1 AGEINT Applied to ICS and Cyber-Physical Intelligence permitted defensive utility: curriculum uses and safe outputs

Evidence anchor. Section 67; [255, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**.

67.3.6.2 AGEINT Applied to ICS and Cyber-Physical Intelligence excluded operational boundary: blocked actions and stop rules

Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [255, 2026]; [256, 2026] and **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

67.3.7 AGEINT Applied to ICS and Cyber-Physical Intelligence governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 67; [255, 2026].

Governance is practiced as a gate on the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane. Learners use the **Cyber-Physical Readiness Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**.

67.3.7.1 AGEINT Applied to ICS and Cyber-Physical Intelligence governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [255, 2026]; [256, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **ICS/OT Cyber-Physical Defense and Tabletop Readiness** failure modes and the **Cyber-Physical Readiness Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

67.3.7.2 AGEINT Applied to ICS and Cyber-Physical Intelligence evidence package handoff: appendices, records, and reuse

Evidence anchor. Section 67; [255, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Cyber-Physical Readiness Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**.

67.3.7.3 AGEINT Applied to ICS and Cyber-Physical Intelligence current-source assurance: verified anchors and local artifact fit

The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**. [255, 2026]; [256, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_nist_csf_2` for **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**?	The NIST Cybersecurity Framework (CSF) 2.0; lane `ics_ot_defense`; checked 2026-05-21.	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric; Official cybersecurity-risk governance framework that adds the Govern function and supplies a common language for AI, OT, and enterprise risk.
What does the module inherit from `official_nist_sp_800_160r1` for **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**?	Engineering Trustworthy Secure Systems, NIST SP 800-160 Vol. 1 Rev. 1; lane `ics_ot_defense`; checked 2026-05-21.	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric; Systems-security engineering foundation for trustworthy systems in contested operational environments and related training programs.
What does the module inherit from `official_nist_sp_800_82r3` for **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**?	Guide to Operational Technology Security, NIST SP 800-82 Rev. 3; lane `source_quality_spine`; checked 2026-05-21.	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric; Official NIST operational technology security guidance.
What does the module inherit from `official_isa_iec_62443` for **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**?	ISA/IEC 62443 Series of Standards; lane `source_quality_spine`; checked 2026-05-21.	tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric; Official ISA overview of industrial automation and control security standards.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 67; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

67.3.8 AGEINT Applied to ICS and Cyber-Physical Intelligence assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 67; [255, 2026].

67.3.9 AGEINT Applied to ICS and Cyber-Physical Intelligence assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 67; [255, 2026].

67.3.9.1 AGEINT Applied to ICS and Cyber-Physical Intelligence capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation** and [255, 2026]; [256, 2026].

67.3.9.2 AGEINT Applied to ICS and Cyber-Physical Intelligence instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation** and [255, 2026]; [256, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

67.3.9.3 AGEINT Applied to ICS and Cyber-Physical Intelligence assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
AI-Driven Anomaly Detection in OT Networks	Completed **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
LLM Agents for ICS Log Analysis and Threat Correlation	Completed **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
ICS defensive coverage and safety tabletop using synthetic process records	Completed **tabletop packet with OT asset inventory, architecture record, consequences, injects, and debrief rubric** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

67.3.10 AGEINT Applied to ICS and Cyber-Physical Intelligence refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [255, 2026]; [256, 2026] and **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**.

67.3.10.1 AGEINT Applied to ICS and Cyber-Physical Intelligence refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**. The local signals begin with [255, 2026]; [256, 2026].

67.3.10.2 AGEINT Applied to ICS and Cyber-Physical Intelligence claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**, and the source spine for these checks begins with [255, 2026]; [256, 2026].

67.3.11 AGEINT Applied to ICS and Cyber-Physical Intelligence reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [255, 2026]; [256, 2026].

Triangulation anchors. In module 49's review-checklist section, directly verified anchors for the **ICS/OT Cyber-Physical Defense and Tabletop Readiness** lane include [of Standards and Technology, 2024f]; [of Standards and Technology, 2022b]; [of Standards and Technology, 2024b]; [of Automation, 2026]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation**. [255, 2026]; [256, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.

- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

67.3.12 AGEINT Applied to ICS and Cyber-Physical Intelligence learning-path links: module map, overview, and curriculum atlas

Use the cross-links below to place **AI-Driven Anomaly Detection in OT Networks; LLM Agents for ICS Log Analysis and Threat Correlation** in the wider unit: the orientation sets the frame, the parent unit supplies the shared safety posture, and the neighbouring modules show what evidence enters and leaves. Lead sources: [255, 2026]; [256, 2026].

Section 2, Section 62, Section 66, Section 68

68 LEGAL, ETHICAL, AND OVERSIGHT FRAMEWORKS

68.1 LEGAL, ETHICAL, AND OVERSIGHT FRAMEWORKS learning spine and source route: unit purpose, module order, and evidence handoff

Evidence anchor. Section 68; [234, 2026].

68.1.1 authority, rights, oversight, and auditability discipline spine: domain question and learning focus

Evidence anchor. Section 68; [234, 2026].
This unit teaches **authority, rights, oversight, and auditability**. Legal and ethics lessons make authority, proportionality, privacy, transparency, redress, audit trails, and public accountability design constraints.

68.1.2 authority, rights, oversight, and auditability source-use contract: citation roles and evidence limits

Evidence anchor. Section 68; [234, 2026].
Use directive, public-sector AI, and agentic AI anchors for authority mapping, transparency, records, and rights-impact claims.

68.1.3 authority, rights, oversight, and auditability practice artifact: recurring packet and retained evidence

Evidence anchor. Section 68; [234, 2026].
The recurring practice artifact is a **authority-and-impact review register** that draws on authority map, rights-impact note, audit log, and redress or escalation path. The unit keeps its learning spine explicit. Learners map authority, affected groups, oversight owner, audit evidence, and redress path before release.

68.1.4 authority, rights, oversight, and auditability safety boundary: accountable, synthetic, and evidence-bounded limits

Capability never substitutes for legal authority, accountable review, affected-person safeguards, or auditability.
This unit introduces the part's governing question, evidence artifacts, source-support spine, and capstone thread before the individual modules begin. [234, 2026]; [238, 2026].
Learners carry one unit capstone thread through the part: define an accountable intelligence question, bind it to source-quality constraints, produce a reviewable artifact, test the artifact against failure modes, and hand it off with enough context for another analyst or instructor to audit. The capstone remains public, synthetic, or owned-lab throughout; its first source anchors are [234, 2026]; [238, 2026].
This unit's deliverables are a source-canon card, claim/evidence ledger, safe-practice lab packet, failure-mode note, instructor rubric, and debrief memo. The full source-lane and evidence-package ledgers appear in the orientation and appendices; this unit introduction keeps only the learner-facing spine for [234, 2026]; [238, 2026].
This unit's safety gates are scope authorization, rights review, data provenance, tool allowlisting, human oversight, rollback, and evidence-bounded output. A missing gate turns the activity into a tabletop, audit, or written governance exercise until the gate is restored against [234, 2026]; [238, 2026].
Capstone thread:

Phase	Artifact	Review gate
Question	accountable learning question and excluded-action list	instructor confirms scope, allowed data, and rights impact
Source canon	source-lane map with guide citations, verified anchors, and refresh dates	citation keys resolve and source identity lock remains stable
Evidence ledger	claim, evidence, uncertainty, confidence, and reviewer register	every material claim has a source, caveat, and owner
Safe lab	synthetic or public dataset packet, tool allowlist, and stop conditions	no live target, private data, external action, or unsafe cyber-physical step
Assurance	evaluation rubric, failure-mode drill, rights map, and remediation note	human reviewer signs off before presentation or reuse
Debrief	capstone memo with lessons, residual risk, refresh triggers, and handoff owner	all unresolved questions and future approvals are explicit

Research lane: Legal, Ethical, and Oversight Architecture. Core anchors: [Archives and Administration, 1981]; [Agency, 2026g]; [Union, 2024]. Conceptual focus: turning authority, accountability, transparency, and review into design constraints rather than post-hoc paperwork. Composability contract: policies, approvals, audit logs, evidence, and action permissions remain linked but independently inspectable. **Practice lens:** Oversight-and-Rights Lens; Which authority, impact assessment, public-register entry, audit record, and escalation path must exist before the workflow is allowed? [234, 2026]; [238, 2026].

68.1.5 LEGAL, ETHICAL, AND OVERSIGHT FRAMEWORKS visual navigation and module map: evidence flow, order, and safety cues

The unit uses Figure 143 and Figure 144 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 67, Section 69.

68.1.6 LEGAL, ETHICAL, AND OVERSIGHT FRAMEWORKS module roster and source-lane inventory: citations, lanes, and learner route

Module	Section reference	Source spine
Legal Authorities and Constraints	Section 69	[234, 2026]; [238, 2026]; [241, 2026]; [276, 2026]; [277, 2026]; [284, 2026]; [288, 2026]; [289, 2026]; [293, 2026]; [221, 2026]; [006, 2026]; [222, 2026]; [298, 2026]; [297, 2026].
Ethics of Intelligence and Cognitive Security	Section 70	[238, 2026]; [239, 2026]; [240, 2026]; [278, 2026]; [279, 2026]; [283, 2026]; [290, 2026]; [291, 2026]; [294, 2026]; [172, 2026]; [298, 2026]; [297, 2026].

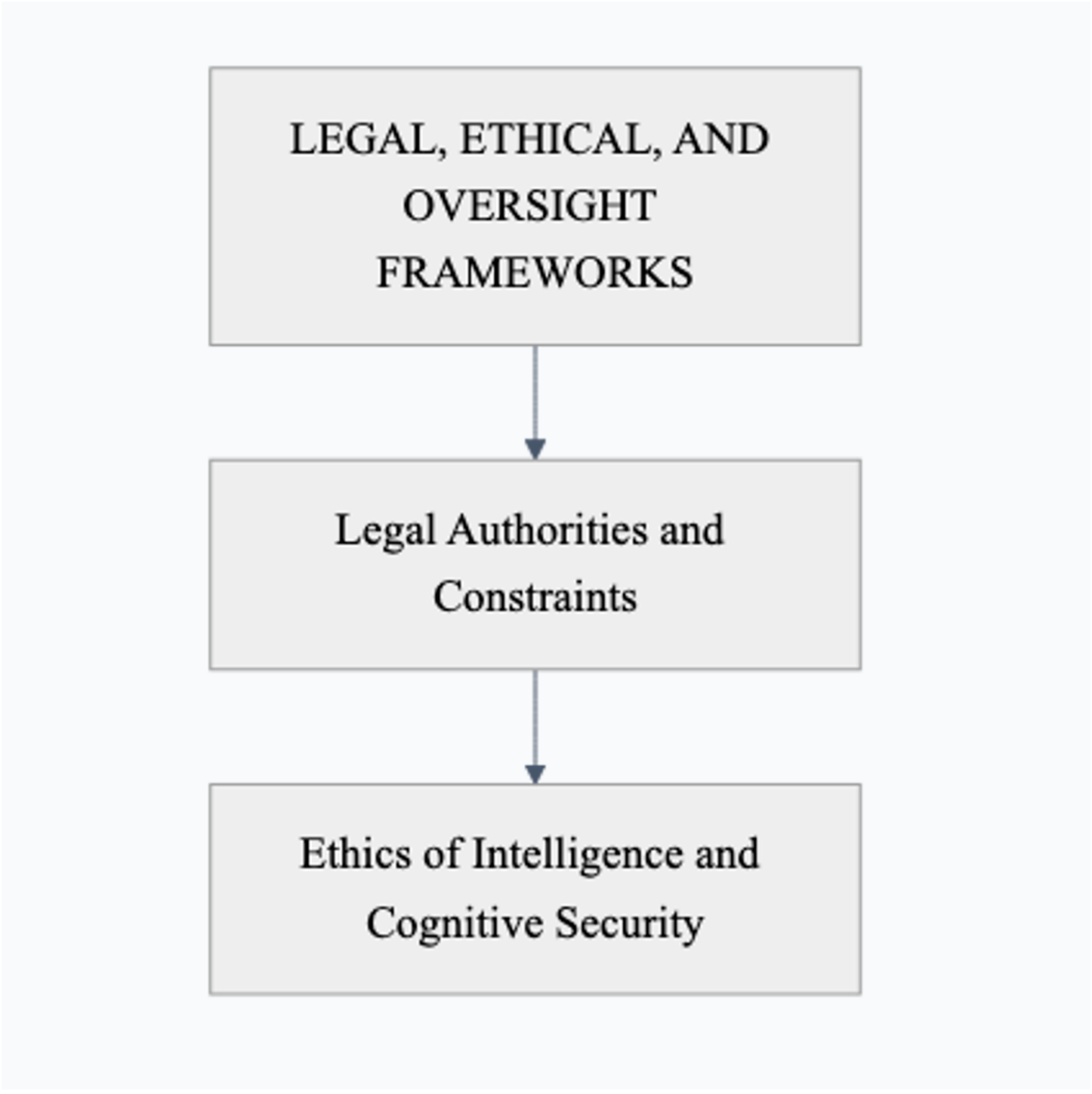


Figure 143: The unit module map traces the part's chapters as a linear reading sequence. It is anchored to the legal ethical and oversight frameworks section; use it to inspect 2 module nodes in the unit's ordered, source-backed reading sequence from its first module to its last while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

Figure 144: This part treats authority, proportionality, rights impact, accountable oversight, audit trail, transparency, and redress as a sequential gate ladder that any proposed capability must clear, with the legal and ethics chapters mapping authority and defining the duties that bind each gate.

69 Legal Authorities and Constraints

69.0.1 Legal Authorities and Constraints figures and course links: visual evidence, source flow, and navigation

The module uses Figure 145 and Figure 143 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 68, Section 70.
This module teaches the **Legal, Ethical, and Oversight Architecture** lane through a bounded, source-backed coursebook chapter. [234, 2026]; [238, 2026].

69.1 Legal, Ethical, and Oversight Architecture frame for Legal Authorities and Constraints: source context, topic focus, and reader task

Evidence anchor. Section 69; [234, 2026].

69.1.1 Legal Authorities and Constraints orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 69; [234, 2026].

69.1.2 Legal Authorities and Constraints conceptual primer: source context, core model, and reader task

This chapter teaches legal and oversight architecture as design constraint: authority, rights, auditability, proportionality, transparency, and redress shape what work may proceed. The chapter uses **Oversight-and-Rights Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**.
The central distinction is to separate having a capability from having authority and accountable review. Core topics include **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law; Intelligence Community Directives: Full Index (IRP/FAS)**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.
Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Archives and Administration, 1981]; [Agency, 2026g]; [Union, 2024]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [234, 2026]; [238, 2026].
Learners move from vocabulary and the **Oversight-and-Rights Lens** distinction through topic lessons on **Executive Order 12333: United States Intelligence Activities** with evidence and misconception checks, then assemble an **authority-and-impact register with approvals, limits, public notice, audit owners, and review dates** with safety and rights gates.

69.1.3 Legal Authorities and Constraints learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 69; [234, 2026].

- Connect **Executive Order 12333: United States Intelligence Activities and FISA and Surveillance Law** to **Legal, Ethical, and Oversight Architecture** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build an **authority-and-impact register with approvals, limits, public notice, audit owners, and review dates** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate having a capability from having authority and accountable review; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as authority laundering through tools, missing audit trails, privacy overreach, and treating governance as a static checklist, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: governance content supports lawful design, education, and review; it does not justify unauthorized collection or deployment.

69.1.4 Legal Authorities and Constraints core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 69; [234, 2026].

Term	Working definition
Authority	the legal, institutional, or classroom basis for an activity
Proportionality	the test that a method is no more intrusive than the need justifies
Oversight	independent review that can challenge or constrain the activity
Redress	a path for affected people to contest or correct harm
Audit trail	retained evidence that enables later review of decisions and outputs
Executive Order 12333: United States…	Key terms: Executive, Order, United.
FISA and Surveillance Law	Key terms: FISA, Surveillance, Law.

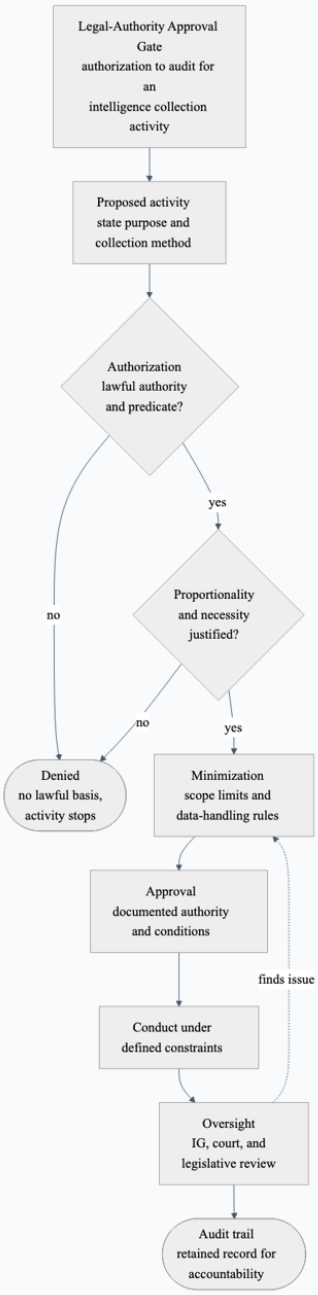


Figure 145: This diagram teaches the sequence of legal checkpoints that gate an intelligence activity, from lawful authorization and proportionality through minimization, approval, oversight, and a retained audit trail. The captioned view belongs to the legal ethical and oversight frameworks / legal authorities and constraints section and should be read as a map of Legal-Authority Approval Gate authorization to audit for an intelligence collection activity, Proposed activity state purpose and collection method, Denied no lawful basis, activity stops, and Minimization scope limits and data-handling rules, not as a capability score or live-task instruction.

69.2 Oversight-and-Rights Lens path for Legal Authorities and Constraints: lesson cluster, safe artifact, and review

Evidence anchor. Section 69; [234, 2026].

69.2.1 Legal Authorities and Constraints practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 69; [234, 2026].

69.2.2 Legal Authorities and Constraints topic lessons: source-backed concepts and transfer tasks

This module builds legal and oversight architecture as design constraint: authority, rights, auditability, proportionality, transparency, and redress shape what work may proceed. The sequence opens with **Executive Order 12333: United States Intelligence Activities**, **FISA and Surveillance Law**, **Intelligence Community Directives: Full Index (IRP/FAS)** and applies the **Oversight-and-Rights Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 143; module overview Section 69; curriculum atlas Section 2.

Triangulation anchors. In module 50's topic-lessons section, directly verified anchors for the **Legal, Ethical, and Oversight Architecture** lane include [Archives and Administration, 1981]; [Agency, 2026g]; [Union, 2024]; [of Europe, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

69.2.2.1 Lesson 1: Executive Order 12333: United States Intelligence Activities

Concept. Executive Order 12333: United States Intelligence Activities maps the legal source to authority, oversight, retention, and redress fields before any workflow is allowed.

Why it matters. Executive Order 12333 connects classroom vocabulary to Legal, Ethical, and Oversight Architecture practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Executive Order 12333: United States Intelligence Activities rests on [221, 2026]. Its anchor reference records: Presidential Policy Directive 28 (PPD-28), Signals Intelligence Activities, in the ODNI IC Legal Reference Book, establishing principles and safeguards (data minimization and protections for personal information regardless of nationality) that govern U.S. Use it for the claim that **Executive Order 12333: United States Intelligence Activities** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Archives and Administration, 1981]; [Agency, 2026g].

Evidence to inspect. Ground **Executive Order 12333** in the evidence the row cites. [221, 2026] Presidential Policy Directive 28 (PPD-28), Signals Intelligence Activities, in the ODNI IC Legal Reference Book, establishing principles and safeguards (data minimization and protections for personal information regardless of nationality) that govern U.S. signals intelligence collection and use. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Executive Order 12333**, build a **authority-and-impact register with approvals, limits, public notice, audit owners, and review dates** for this authority mapping and rights-aware release review topic. The artifact must name the source descriptor, the bounded claim about **Executive Order 12333**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Executive Order 12333** work as an **authority-and-impact review register** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **Executive Order 12333**: that a legal source grants authority without scope and oversight.

Transfer task. Transfer **Executive Order 12333** to a second module by preserving authority mapping and rights-aware release review, changing the source evidence, and naming a new reviewer.

69.2.2.2 Lesson 2: FISA and Surveillance Law

Concept. FISA and Surveillance Law maps the legal source to authority, oversight, retention, and redress fields before any workflow is allowed.

Why it matters. Without explicit treatment of **FISA and Surveillance Law**, authority laundering through tools undermines authority mapping and rights-aware release review; the lesson builds the habit to separate having a capability from having authority and accountable review.

Source support. FISA and Surveillance Law rests on [298, 2026] and [297, 2026]. The closest source to this row notes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for the working definition that **FISA and Surveillance Law** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Archives and Administration, 1981]; [Agency, 2026g].

Evidence to inspect. For **FISA and Surveillance Law**, work from the cited evidence behind this row. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. Build a **authority-and-impact register with approvals, limits, public notice, audit owners, and review dates** for this authority mapping and rights-aware release review topic. The artifact must name the source descriptor, the bounded claim about **FISA and Surveillance Law**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape this subject work as an **authority-and-impact review register** that records its evidence, the residual uncertainty, the named reviewer, and the stop condition.

Misconception check. Correct the misconception about **FISA and Surveillance Law**: that a legal source grants authority without scope and oversight.

Transfer task. Transfer **FISA and Surveillance Law** to a second module by preserving authority mapping and rights-aware release review, changing the source evidence, and naming a new reviewer.

69.2.2.3 Lesson 3: Intelligence Community Directives: Full Index (IRP/FAS)

Concept. Intelligence Community Directives: Full Index (IRP/FAS) maps the theory to institutions: priorities, feedback, incentives, review loops, and records shape what an intelligence community notices and ignores.

Why it matters. Intelligence Community Directives connects classroom vocabulary to Legal, Ethical, and Oversight Architecture practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. Intelligence Community Directives: Full Index (IRP/FAS) rests on [006, 2026]. Its anchor reference records: ICDs are the principal means by which the DNI provides policy, guidance, and direction to the U.S. Use it for the working definition that **Intelligence Community Directives: Full Index (IRP/FAS)** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Archives and Administration, 1981]; [Agency, 2026g].

Evidence to inspect. Ground **Intelligence Community Directives** in the evidence the row cites. [006, 2026] A Federation of American Scientists repository cataloguing the Intelligence Community Directives (ICDs) issued by the Director of National Intelligence. ICDs are the principal means by which the DNI provides policy, guidance, and direction to the U.S. Intelligence Community. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Intelligence Community Directives**, build an institutional feedback-loop map with incentives, review points, and oversight hooks. Shape **Intelligence Community Directives** work as an **authority-and-impact review register** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that Intelligence Community Directives: Full Index (IRP/FAS) can be used while ignoring the rule to separate having a capability from having authority and accountable review.

Transfer task. Transfer **Intelligence Community Directives** to a second module by preserving authority mapping and rights-aware release review, changing the source evidence, and naming a new reviewer.

69.2.2.4 Lesson 4: CIA Classification Guide (National Archives)

Concept. CIA Classification Guide (National Archives) studies the declassified record for institutional lessons about oversight, source protection, and limits on translating history into practice.

Why it matters. CIA Classification Guide (National Archives) matters in the **Legal, Ethical, and Oversight Architecture** lane because authority mapping and rights-aware release evidence must stay separate from judgment; authority laundering through tools is a common failure.

Source support. CIA Classification Guide (National Archives) rests on [222, 2026]. The most specific cited work observes: The scope of the CIA mission is vast and the complexities of intelligence tradecraft. Use it for pinning down the scope of **CIA Classification Guide (National Archives)**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Archives and Administration, 1981]; [Agency, 2026g].

Evidence to inspect. For **CIA Classification Guide (National Archives)**, work from the cited evidence behind this row. [222, 2026] The scope of the CIA mission is vast and the complexities of intelligence tradecraft. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **CIA Classification Guide (National Archives)**, build a **authority-and-impact register with approvals, limits, public notice, audit owners, and review dates** for this authority mapping and rights-aware release review topic. The artifact must name the source descriptor, the bounded claim about **CIA Classification Guide**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape this subject work as an **authority-and-impact review register** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that CIA Classification Guide (National Archives) is optional whenever separate having a capability from having authority and accountable review feels inconvenient.

Transfer task. Transfer **CIA Classification Guide (National Archives)** to a second module by preserving authority mapping and rights-aware release review, changing the source evidence, and naming a new reviewer.

69.2.2.5 Lesson 5: Allied Legal Frameworks: RIPA, Investigatory Powers Act, GDPR

Concept. Allied Legal Frameworks: RIPA, Investigatory Powers Act, GDPR compares allied legal frameworks by authority scope, retention, redress, and proportionality—not by capability alone.

Why it matters. Analysts use **Allied Legal Frameworks** to separate having a capability from having authority and accountable review. A defensible treatment names the judgment it enables for authority mapping and rights-aware release review, the proof limit that authority laundering through tools would otherwise hide, and the reviewer accountable for challenge.

Source support. Allied Legal Frameworks: RIPA, Investigatory Powers Act, GDPR rests on [298, 2026] and [297, 2026]. Its anchor reference records: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for the working definition that **Allied Legal Frameworks: RIPA, Investigatory Powers Act, GDPR** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Archives and Administration, 1981]; [Agency, 2026g].

Evidence to inspect. Ground **Allied Legal Frameworks** in the evidence the row cites. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **Allied Legal Frameworks**, build a **authority-and-impact register with approvals, limits, public notice, audit owners, and review dates** for this authority mapping and rights-aware release review topic. The artifact must name the source descriptor, the bounded claim about **Allied Legal Frameworks**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **Allied Legal Frameworks** work as an **authority-and-impact review register** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception that Allied Legal Frameworks: RIPA, Investigatory Powers Act, GDPR establishes intent without reviewing alternative explanations.

Transfer task. Transfer **Allied Legal Frameworks** to a second module by preserving authority mapping and rights-aware release review, changing the source evidence, and naming a new reviewer.

69.2.2.6 Lesson 6: The International Law of Intelligence

Concept. The International Law of Intelligence applies International, Law within Legal, Ethical, and Oversight Architecture: learners use separate having a capability from having authority and accountable review and authority mapping and rights-aware release review evidence before any judgment moves forward.

Why it matters. Without explicit treatment of **The International Law of Intelligence**, authority laundering through tools undermines authority mapping and rights-aware release review; the lesson builds the habit to separate having a capability from having authority and accountable review.

Source support. The International Law of Intelligence rests on [298, 2026] and [297, 2026]. Its anchor reference records: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for fixing what **The International Law of Intelligence** covers, marking the boundary it must not cross, and timing the next source refresh. External triangulation uses [Archives and Administration, 1981]; [Agency, 2026g].

Evidence to inspect. Ground **The International Law of Intelligence** in the evidence the row cites. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Each source above earns its place in this topic only when you can state its bounded claim, its provenance, its uncertainty, and the fact that would retire it.

Student artifact. For **The International Law**, build a **authority-and-impact register with approvals, limits, public notice, audit owners, and review dates** for this authority mapping and rights-aware release review topic. The artifact must name the source descriptor, the bounded claim about **International Law of Intelligence**, the caveat that limits it, the uncertainty note, the out-of-scope-use boundary, and the reviewer accountable for challenge. Shape **The International Law of Intelligence** work as an **authority-and-impact review register** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception that The International Law of Intelligence replaces human review whenever evidence looks plausible.

Transfer task. Transfer **The International Law of Intelligence** to a second module by preserving authority mapping and rights-aware release review, changing the source evidence, and naming a new reviewer.

69.2.3 Legal Authorities and Constraints worked safe example: synthetic inputs, evidence, and review

Worked example: a sample agency training team reviews whether a classroom AI workflow is allowed. [234, 2026]; [238, 2026].

Triangulation anchors. In module 50's worked-example section, directly verified anchors for the **Legal, Ethical, and Oversight Architecture** lane include [Archives and Administration, 1981]; [Agency, 2026g]; [Union, 2024]; [of Europe, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **authority, rights, oversight, and auditability**. Learners use a **authority-and-impact review register** and keep this boundary visible: Capability never substitutes for legal authority, accountable review, affected-person safeguards, or auditability.

Frame. The classroom question centers on **Executive Order 12333: United States Intelligence Activities**. Excluded actions stay explicit, and the **Oversight-and-Rights Lens** planning question is: Which authority, impact assessment, public-register entry, audit record, and escalation path must exist before the workflow is allowed?

Inputs. For the **Executive Order 12333: United States Intelligence Activities** scenario, use public policy excerpts, synthetic workflow notes, a rights-impact checklist, and an audit-log template. The Oversight-and-Rights Lens intake note records provenance, sensitivity, fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Executive Order 12333: United States Intelligence Activities**, students map authority, test proportionality, name affected groups, assign oversight, and define redress or escalation. Pause whenever an inference about Executive Order 12333: United States Intelligence Activities appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Executive Order 12333: United States Intelligence Activities** classroom scenario; unit artifact = authority-and-impact review register; evidence = allowed inputs; method = authority mapping and rights-aware release review; output = an authority-and-impact register with approvals, limits, audit owner, and review date; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Executive Order 12333: United States Intelligence Activities** as "Oversight-and-Rights Lens confirms it" is not enough. The revision ties the claim to authority mapping and rights-aware release review, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Executive Order 12333: United States Intelligence Activities** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

69.2.4 Legal Authorities and Constraints practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Oversight-and-Rights Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**.

Triangulation anchors. In module 50's practice-sequence section, directly verified anchors for the **Legal, Ethical, and Oversight Architecture** lane include [Archives and Administration, 1981]; [Agency, 2026g]; [Union, 2024]; [of Europe, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Executive Order 12333: United States Intelligence Activities, FISA and Surveillance Law, Intelligence Community Directives: Full Index; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Legal, Ethical, and Oversight Architecture** lane.
2. Frame	Answer the lens question: Which authority, impact assessment, public-register entry, audit record, and escalation path must exist before the workflow is allowed?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Executive Order 12333: United States Intelligence Activities: authority-and-impact register with approvals, limits, public notice, audit owners, and review dates.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the authority-and-impact review register fields for Executive Order 12333: United States Intelligence Activities.	Unit profile note.	Evidence artifacts include authority map, rights-impact note.
4. Challenge	Test the misconception that a legal source grants authority without scope and oversight.	Failure-mode note.	The artifact applies the key distinction: separate having a capability from having authority and accountable review.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

69.2.4.1 Legal Authorities and Constraints instructor notes: source reasoning, review points, and studio focus

Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**. [234, 2026]; [238, 2026].

69.2.4.2 Legal Authorities and Constraints extension exercise: peer validation and refresh trigger review

Evidence anchor. Section 69; [234, 2026].

Have learners swap artifacts and apply the **Oversight-and-Rights Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**.

69.2.5 Legal Authorities and Constraints knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 69; [234, 2026].

1. Explain how **Executive Order 12333: United States Intelligence Activities** is defined here; name the source descriptor that supports the definition.

2. Contrast **Executive Order 12333: United States Intelligence Activities** with **FISA and Surveillance Law** using the **Oversight-and-Rights Lens** artifact fields.
3. Identify one failure mode from the **Legal, Ethical, and Oversight Architecture** lane and the evidence that would reveal it.
4. Answer the coursebook review question: What control turns a capability into an accountable, reviewable workflow?
5. Correct this misconception: that a legal source grants authority without scope and oversight.

69.2.5.1 Legal Authorities and Constraints answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Executive Order 12333: United States Intelligence Activities** without source evidence, uncertainty, or a safe transfer task.

69.3 Legal Authorities and Constraints assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 69; [234, 2026].

69.3.1 Legal Authorities and Constraints evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 69; [234, 2026].

69.3.2 Legal Authorities and Constraints transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 69; [234, 2026].

69.3.2.1 Legal Authorities and Constraints lineage and source tradition: profile, concepts, and first anchors This sits in the **Legal, Ethical, and Oversight Architecture** lineage: turning authority, accountability, transparency, and review into design constraints rather than post-hoc paperwork. [234, 2026]; [238, 2026].

69.3.2.2 Legal Authorities and Constraints working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 69; [234, 2026].
The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**, with provenance and reviewability throughout.

69.3.2.3 Legal Authorities and Constraints knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** legal authorities, policy constraints, affected groups, retention duties, oversight roles, and audit logs. [234, 2026]; [238, 2026].
- **Transforms:** authority mapping, proportionality review, rights-impact assessment, redress planning, and escalation routing.
- **Outputs:** authority-and-impact register, audit trail, redress note, and unresolved-risk owner.
- **Failure modes:** authority laundering, missing audit trails, privacy overreach, and governance-as-afterthought.

69.3.2.4 Legal Authorities and Constraints transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 69; [234, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**.
- **Evidence contract:** keep the **Legal, Ethical, and Oversight Architecture** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as authority-and-impact register, audit trail, redress note, and unresolved-risk owner that another reviewer can audit.

69.3.2.5 Legal Authorities and Constraints profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 69; [234, 2026].
The matched profile emphasizes turning authority, accountability, transparency, and review into design constraints rather than post-hoc paperwork. The method stack is authority mapping, role assignment, impact assessment, documentation review, escalation triggers, and independent oversight; the local topic cluster is **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**.

69.3.3 Legal Authorities and Constraints evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 69; [234, 2026].
Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Legal, Ethical, and Oversight Architecture** profile tells reviewers what evidence is strong enough for the module artifact built around **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**.

69.3.3.1 Legal Authorities and Constraints guide source spine: inherited keys and local citation roles Primary guide citations: [234, 2026]; [238, 2026]; [241, 2026]; [276, 2026]; [277, 2026]; [284, 2026]; [288, 2026]; [289, 2026]; [293, 2026]; [221, 2026]; [006, 2026]; [222, 2026]; [298, 2026]; [297, 2026].

69.3.3.2 Legal Authorities and Constraints verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [234, 2026]; [238, 2026].

Tier	What counts	How it is used
Source guide	[234, 2026]; [238, 2026]; [241, 2026]; [276, 2026]; [277, 2026]; [284, 2026]; [288, 2026]; [289, 2026]; [293, 2026]; [221, 2026]; [006, 2026]; [222, 2026]; [298, 2026]; [297, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 50's source-canon section, directly verified anchors for the **Legal, Ethical, and Oversight Architecture** lane include [Archives and Administration, 1981]; [Agency, 2026g]; [Union, 2024]; [of Europe, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Maintenance rule: Perplexity may suggest candidates for **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law** and [234, 2026]; [238, 2026], but only directly verified source URLs are encoded as citations.

69.3.3.3 Legal Authorities and Constraints intelligence practice lens: evidence artifact and safety check Practice lens: **Oversight-and-Rights Lens** for **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**. [234, 2026]; [238, 2026].

Planning question: Which authority, impact assessment, public-register entry, audit record, and escalation path must exist before the workflow is allowed?

Evidence artifact: authority-and-impact register with approvals, limits, public notice, audit owners, and review dates.

Validation rule: confirm lawful purpose, proportionality, retention, review, and appeal or redress paths. Applied to **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**.

Handoff contract: handoff includes approvals, policy constraints, audit evidence, and unresolved legal or ethical issues.

Safety check: reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought.

69.3.3.4 Legal Authorities and Constraints runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 69; [234, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	50.99	50.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Legal Authorities and Constraints to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
Bounded autonomy, procurement, incident-response, and assurance studio	50.101	50.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Legal Authorities and Constraints	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
Model-card, recoverability, retention, and learner-support evidence package	50.102	50.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Legal Authorities and Constraints	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
Executive Order 12333: United States Intelligence Activities	50.1	50.1 Executive Order 12333: United States Intelligence Activities	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
FISA and Surveillance Law	50.2	50.2 FISA and Surveillance Law	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
Intelligence Community Directives: Full Index (IRP/FAS)	50.3	50.3 Intelligence Community Directives: Full Index (IRP/FAS)	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
CIA Classification Guide (National Archives)	50.4	50.4 CIA Classification Guide (National Archives)	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
Allied Legal Frameworks: RIPA, Investigatory Powers Act, GDPR	50.5	50.5 Allied Legal Frameworks: RIPA, Investigatory Powers Act, GDPR	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
The International Law of Intelligence	50.6	50.6 The International Law of Intelligence	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought

69.3.3.5 Legal Authorities and Constraints reusable subsection contract: topic rows, artifacts, and safety duties Evidence anchor. Section 69; [234, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Executive Order 12333: United States Intelligence Activities	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
FISA and Surveillance Law	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
Intelligence Community Directives: Full Index (IRP/FAS)	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
CIA Classification Guide (National Archives)	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
Allied Legal Frameworks: RIPA, Investigatory Powers Act, GDPR	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
The International Law of Intelligence	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought

69.3.3.6 Legal Authorities and Constraints annotated source ledger: real titles and local contribution Each source cited by this **Legal, Ethical, and Oversight Architecture** module is paired below with its real title and a one-line note on what it contributes to **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**.

Source	Cited work	What it contributes	Status
[234, 2026]	AI Act	The European Commission's official page on the AI Act, described as the first comprehensive legal framework on artificial intelligence worldwide. It explains the regulation's risk-based approach, classifying AI systems into unacceptable, high, transparency, and minimal risk tiers, with prohibited practices and strict requirements for high-risk uses.	verified source-guide

Source	Cited work	What it contributes	Status
[238, 2026]	Recommendation on the Ethics of Artificial Intelligence	The official UNESCO page for the Recommendation on the Ethics of Artificial Intelligence, the first global standard-setting instrument on AI ethics, adopted in 2021 and applicable to all 194 member states. It outlines four core values, including human rights protection and environmental flourishing, and ten guiding principles such as proportionality, privacy, transparency, and fairness.	verified source-guide
[241, 2026]	Modernised Convention 108	Official Council of Europe Convention 108+ source.	original source-guide
[276, 2026]	What is a Data Protection Impact Assessment and When Is This Mandatory?	A European Data Protection Board FAQ page, part of its data protection guide for small businesses, explaining Data Protection Impact Assessments (DPIAs) and when they are mandatory. It describes a DPIA as a written assessment of the impact of a planned processing operation, required when processing poses high risks to individuals' rights.	verified source-guide
[277, 2026]	Endorsed WP29 Guidelines	This is a European Data Protection Board webpage listing guidelines and documents originating from the Article 29 Working Party that the EDPB endorsed at its first plenary meeting. The catalogued materials relate to the GDPR and cover topics such as consent and transparency, data breach notification, automated decision-making and profiling, data protection impact assessments, data protection officers, and binding corporate rules.	verified source-guide
[284, 2026]	Verifiable Credential Data Integrity 1.0	The W3C Recommendation for Verifiable Credential Data Integrity 1.0, published May 2025, defining mechanisms for ensuring the authenticity and integrity of verifiable credentials using cryptographic proofs. It specifies a process of data transformation, hashing, and proof generation, and a corresponding verification procedure, along with a proof data model containing properties such as type, verification method, purpose, and proof value.	verified source-guide
[288, 2026]	Algorithmic Transparency Recording Standard Hub	A GOV.UK collection page serving as the hub for the UK Algorithmic Transparency Recording Standard (ATRS), maintained by the Government Digital Service. It provides a standardized template for documenting public-sector use of algorithmic tools, completion guidance, policy on scope and compliance, and a searchable repository of published transparency records.	verified source-guide

Source	Cited work	What it contributes	Status
[289, 2026]	Guidance for Organisations Using the Algorithmic Transparency Recording Standard	This is a GOV.UK guidance page published by the Government Digital Service that instructs public sector organizations on completing the Algorithmic Transparency Recording Standard (ATRS) template and publishing their records to the GOV.UK repository. It applies both to central government bodies required to publish under mandatory policy and to other public sector bodies doing so voluntarily.	verified source-guide
[293, 2026]	Inventory of NARA Artificial Intelligence (AI) Use Cases	The National Archives and Records Administration (NARA) official inventory of its artificial intelligence use cases, documenting 14 projects across deployed, pilot, and planned stages. Deployed efforts include workplace productivity tools, automated tagging for museum experiences, and historical record retrieval, while pilots cover PII detection and redaction, semantic search, and metadata generation, and planned work targets FOIA processing and public search.	verified source-guide
[221, 2026]	About	Presidential Policy Directive 28 (PPD-28), Signals Intelligence Activities, in the ODNI IC Legal Reference Book, establishing principles and safeguards (data minimization and protections for personal information regardless of nationality) that govern U.S. signals intelligence collection and use.	original source-guide
[006, 2026]	Director of National Intelligence - Intelligence Community Directives	A Federation of American Scientists repository cataloguing the Intelligence Community Directives (ICDs) issued by the Director of National Intelligence. ICDs are the principal means by which the DNI provides policy, guidance, and direction to the U.S. Intelligence Community.	verified source-guide
[222, 2026]	CIA - National Archives	The scope of the CIA mission is vast and the complexities of intelligence tradecraft.	original source-guide
[298, 2026]	Intelligence Community Directives	Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations.	original source-guide
[297, 2026]	Intelligence Community Directive 203: Analytic Standards	Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products.	original source-guide

Where this sits. This module's overview is Section 69; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

69.3.4 Legal Authorities and Constraints governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 69; [234, 2026].

69.3.5 Legal Authorities and Constraints analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 50's governance-boundary section, directly verified anchors for the **Legal, Ethical, and Oversight Architecture** lane include [Archives and Administration, 1981]; [Agency, 2026g]; [Union, 2024]; [of Europe, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.
Research lane: **Legal, Ethical, and Oversight Architecture** for **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**. [234, 2026]; [238, 2026].
Curriculum topic spine: Executive Order 12333: United States Intelligence Activities, **FISA and Surveillance Law**, **Intelligence Community Directives: Full Index (IRP/FAS)**. **Verified anchor cluster:** [Archives and Administration, 1981]; [Agency, 2026g]; [Union, 2024]; [of Europe, 2024]; [Privacy and Board, 2026]; [Community, 2020b]; [Community, 2020a].
Conceptual depth: turning authority, accountability, transparency, and review into design constraints rather than post-hoc paperwork.
Method stack: authority mapping, role assignment, impact assessment, documentation review, escalation triggers, and independent oversight.
Composability contract: policies, approvals, audit logs, evidence, and action permissions remain linked but independently inspectable.
Known failure modes: authority laundering through tools, missing audit trails, privacy overreach, and treating governance as a static checklist.
Defensive boundary: governance content supports lawful design, education, and review; it does not justify unauthorized collection or deployment. Applied to **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**.

Anchor	Why it matters here
[Archives and Administration, 1981]	Official legal anchor for intelligence authorities, rights-aware collection, analytic competition, oversight, and source-method protection. Checked as of 2026-05-21; role: curriculum_anchor.
[Agency, 2026g]	Official NSA public explanation of FISA oversight for signals intelligence collection governed by statutory and court-authorized controls. Checked as of 2026-05-21; role: curriculum_anchor.
[Union, 2024]	Official EU Artificial Intelligence Act legal text. Checked as of 2026-05-21; role: source_quality_anchor.
[of Europe, 2024]	Official treaty anchor for human rights, democracy, rule-of-law, risk management, accountability, and public-sector AI governance. Checked as of 2026-05-21; role: curriculum_anchor.
[Privacy and Board, 2026]	Official oversight-report library for privacy, civil-liberties, surveillance, watchlisting, facial-recognition, and redress analysis. Checked as of 2026-05-21; role: curriculum_anchor.
[Community, 2020b]	Official IC principles for lawful, accountable, objective, human-centered, secure, resilient, and science-informed AI. Checked as of 2026-05-21; role: curriculum_anchor.
[Community, 2020a]	Official IC framework for AI goals, authorities, human judgment, bias mitigation, testing, documentation, explainability, and review. Checked as of 2026-05-21; role: curriculum_anchor.

69.3.5.1 Legal Authorities and Constraints evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **Legal, Ethical, and Oversight Architecture** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [234, 2026]; [238, 2026].

69.3.6 Legal Authorities and Constraints agentic boundary: assist, approve, block, and record

Evidence anchor. Section 69; [234, 2026].
AGEINT translation is bounded by the **Legal, Ethical, and Oversight Architecture** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**.

69.3.6.1 Legal Authorities and Constraints permitted defensive utility: curriculum uses and safe outputs

Evidence anchor. Section 69; [234, 2026].
The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**.

69.3.6.2 Legal Authorities and Constraints excluded operational boundary: blocked actions and stop rules

Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [234, 2026]; [238, 2026] and **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

69.3.7 Legal Authorities and Constraints governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 69; [234, 2026].
Governance is practiced as a gate on the **Legal, Ethical, and Oversight Architecture** lane. Learners use the **Oversight-and-Rights Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**.

69.3.7.1 Legal Authorities and Constraints governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [234, 2026]; [238, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Legal, Ethical, and Oversight Architecture** failure modes and the **Oversight-and-Rights Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

69.3.7.2 Legal Authorities and Constraints evidence package handoff: appendices, records, and reuse **Evidence anchor.** Section 69; [234, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Oversight-and-Rights Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**.

69.3.7.3 Legal Authorities and Constraints current-source assurance: verified anchors and local artifact fit The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**. [234, 2026]; [238, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_odni_eo_12333` for **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**?	Executive Order 12333: United States Intelligence Activities; lane `legal_oversight`; checked 2026-05-21.	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates; Official legal anchor for intelligence authorities, rights-aware collection, analytic competition, oversight, and source-method protection.
What does the module inherit from `official_nsa_fisa` for **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**?	Foreign Intelligence Surveillance Act; lane `legal_oversight`; checked 2026-05-21.	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates; Official NSA public explanation of FISA oversight for signals intelligence collection governed by statutory and court-authorized controls.
What does the module inherit from `official_eu_ai_act` for **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**?	Regulation (EU) 2024/1689: Artificial Intelligence Act; lane `source_quality_spine`; checked 2026-05-21.	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates; Official EU Artificial Intelligence Act legal text.
What does the module inherit from `official_council_europe_ai_convention` for **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**?	Framework Convention on Artificial Intelligence; lane `legal_oversight`; checked 2026-05-21.	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates; Official treaty anchor for human rights, democracy, rule-of-law, risk management, accountability, and public-sector AI governance.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 69; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

69.3.8 Legal Authorities and Constraints assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 69; [234, 2026].

69.3.9 Legal Authorities and Constraints assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 69; [234, 2026].

69.3.9.1 Legal Authorities and Constraints capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**.

Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law** and [234, 2026]; [238, 2026].

69.3.9.2 Legal Authorities and Constraints instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law** and [234, 2026]; [238, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

69.3.9.3 Legal Authorities and Constraints assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Executive Order 12333: United States Intelligence Activities	Completed **authority-and-impact register with approvals, limits, public notice, audit owners, and review dates** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
FISA and Surveillance Law	Completed **authority-and-impact register with approvals, limits, public notice, audit owners, and review dates** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
Intelligence Community Directives: Full Index (IRP/FAS)	Completed **authority-and-impact register with approvals, limits, public notice, audit owners, and review dates** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

69.3.10 Legal Authorities and Constraints refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [234, 2026]; [238, 2026] and **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**.

69.3.10.1 Legal Authorities and Constraints refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**. The local signals begin with [234, 2026]; [238, 2026].

69.3.10.2 Legal Authorities and Constraints claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**, and the source spine for these checks begins with [234, 2026]; [238, 2026].

69.3.11 Legal Authorities and Constraints reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [234, 2026]; [238, 2026].

Triangulation anchors. In module 50's review-checklist section, directly verified anchors for the **Legal, Ethical, and Oversight Architecture** lane include [Archives and Administration, 1981]; [Agency, 2026g]; [Union, 2024]; [of Europe, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law**. [234, 2026]; [238, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

69.3.12 Legal Authorities and Constraints learning-path links: module map, overview, and curriculum atlas

Follow the cross-links to move between **Executive Order 12333: United States Intelligence Activities; FISA and Surveillance Law** and the rest of the curriculum without losing the source spine: orientation first, then the parent unit, then the modules on either side. Primary sources: [234, 2026]; [238, 2026].

Section 2, Section 68, Section 70

70 Ethics of Intelligence and Cognitive Security

70.0.1 Ethics of Intelligence and Cognitive Security figures and course links: visual evidence, source flow, and navigation

The module uses Figure 146 and Figure 143 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.

Navigation links: Section 2, Section 68, Section 69, Section 71.

This module teaches the **Legal, Ethical, and Oversight Architecture** lane through a bounded, source-backed coursebook chapter. [238, 2026]; [239, 2026].

70.1 Legal, Ethical, and Oversight Architecture frame for Ethics of Intelligence and Cognitive Security: source context, topic focus, and reader task

Evidence anchor. Section 70; [238, 2026].

70.1.1 Ethics of Intelligence and Cognitive Security orientation: reader task, conceptual primer, outcomes, and vocabulary

Evidence anchor. Section 70; [238, 2026].

70.1.2 Ethics of Intelligence and Cognitive Security conceptual primer: source context, core model, and reader task

This chapter teaches legal and oversight architecture as design constraint: authority, rights, auditability, proportionality, transparency, and redress shape what work may proceed. The chapter uses **Oversight-and-Rights Lens** to connect definitions, evidence tests, practice artifacts, and review gates for **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security**.

The central distinction is to separate having a capability from having authority and accountable review. Core topics include **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security (YorkSpace Dissertation); AI Ethics in Intelligence: Accountability, Transparency, Proportionality**. Each topic covers meaning, evidentiary support, common misconceptions, and safety boundaries.

Governance requirements use verified official, standards, public-domain, or scholarly anchors such as [Archives and Administration, 1981]; [Agency, 2026g]; [Union, 2024]. Technical, theoretical, or empirical statements require direct domain sources and are limited to what those sources establish. [238, 2026]; [239, 2026].

Learners move from vocabulary and the **Oversight-and-Rights Lens** distinction through topic lessons on **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks** with evidence and misconception checks, then assemble an **authority-and-impact register with approvals, limits, public notice, audit owners, and review dates** with safety and rights gates.

70.1.3 Ethics of Intelligence and Cognitive Security learning outcomes: analytic moves, evidence duties, and transfer

Evidence anchor. Section 70; [238, 2026].

- Connect **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks and The Ethics of Cognitive Security (YorkSpace Dissertation)** to **Legal, Ethical, and Oversight Architecture** by naming shared vocabulary, evidence burden, and audience-facing caveats.
- Build an **authority-and-impact register with approvals, limits, public notice, audit owners, and review dates** that keeps observation, inference, uncertainty, source quality, reviewer decision, and refresh trigger separate.
- Apply the key distinction: separate having a capability from having authority and accountable review; show where an apparently useful shortcut would cross that line.
- Diagnose failure modes such as authority laundering through tools, missing audit trails, privacy overreach, and treating governance as a static checklist, then write one recovery move for each failure mode that preserves the learning objective.
- Teach the defensive boundary back to a peer: governance content supports lawful design, education, and review; it does not justify unauthorized collection or deployment.

70.1.4 Ethics of Intelligence and Cognitive Security core vocabulary: source terms, method roles, and safety limits

Evidence anchor. Section 70; [238, 2026].

Term	Working definition
Authority	the legal, institutional, or classroom basis for an activity
Proportionality	the test that a method is no more intrusive than the need justifies
Oversight	independent review that can challenge or constrain the activity
Redress	a path for affected people to contest or correct harm
Audit trail	retained evidence that enables later review of decisions and outputs
Intelligence Ethics: Deontological,...	Key terms: Ethics, Deontological, Consequentialist.
The Ethics of Cognitive Security (YorkSpace...	Key terms: Ethics, Cognitive, Security.

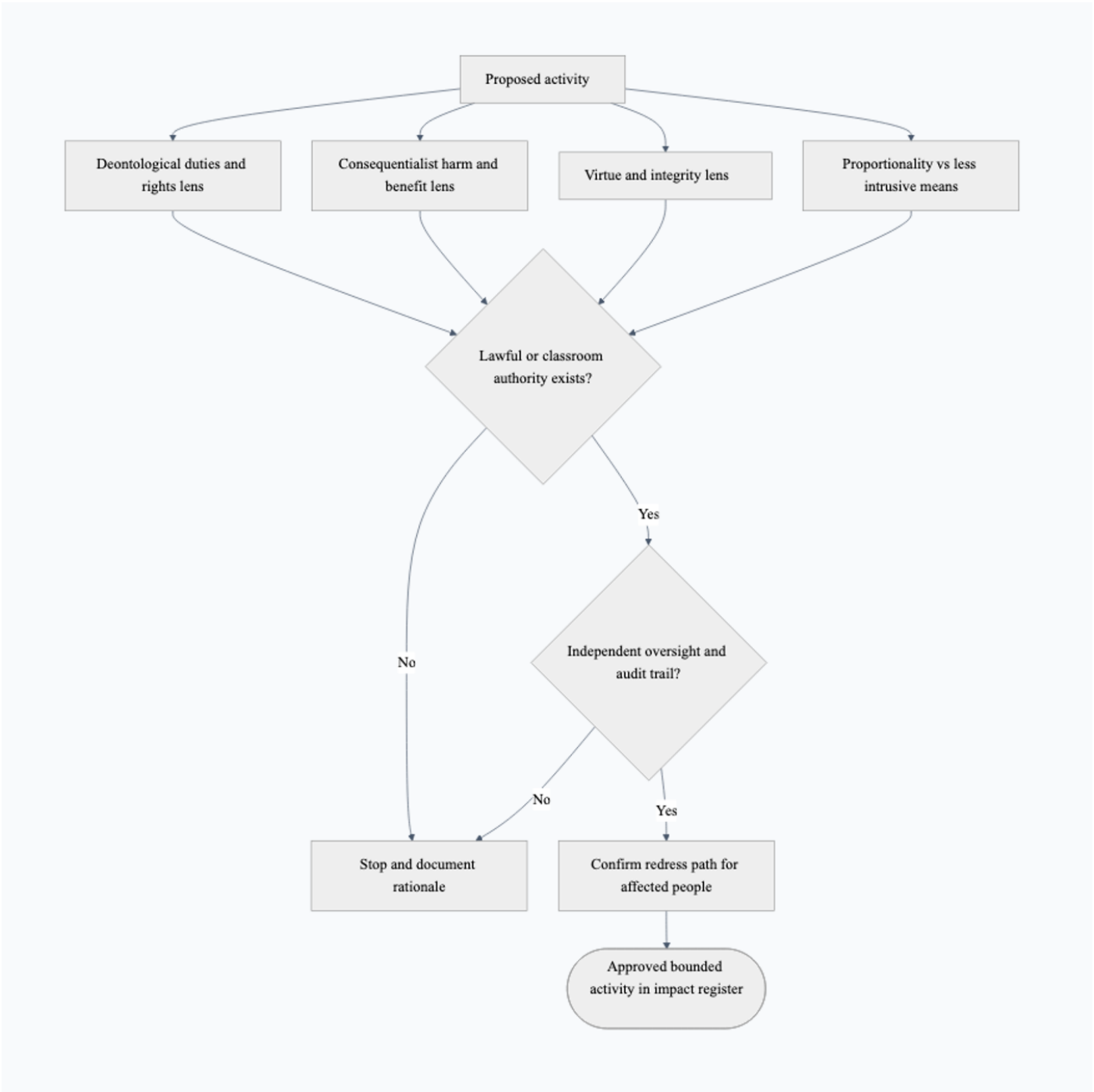


Figure 146: A governance gate that tests a proposed activity for authority, proportionality, rights, oversight, and redress before any work may proceed. Its reader value is to make Proposed activity, Deontological duties and rights lens, Consequentialist harm and benefit lens, and Virtue and integrity lens visible at a glance, with the legal ethical and oversight frameworks / ethics of intelligence and cognitive security section as the source section and defensive review as the boundary.

70.2 Oversight-and-Rights Lens path for Ethics of Intelligence and Cognitive Security: lesson cluster, safe artifact, and review

Evidence anchor. Section 70; [238, 2026].

70.2.1 Ethics of Intelligence and Cognitive Security practice studio: topic lessons, safe worked example, and knowledge check

Evidence anchor. Section 70; [238, 2026].

70.2.2 Ethics of Intelligence and Cognitive Security topic lessons: source-backed concepts and transfer tasks

This module builds legal and oversight architecture as design constraint: authority, rights, auditability, proportionality, transparency, and redress shape what work may proceed. The sequence opens with **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks**, **The Ethics of Cognitive Security (YorkSpace Dissertation)**, **AI Ethics in Intelligence: Accountability, Transparency, Proportionality** and applies the **Oversight-and-Rights Lens** practice frame through concept, evidence, artifact, misconception, and transfer tasks.

Learning-path links. Unit module map Figure 143; module overview Section 70; curriculum atlas Section 2.

Triangulation anchors. In module 51's topic-lessons section, directly verified anchors for the **Legal, Ethical, and Oversight Architecture** lane include [Archives and Administration, 1981]; [Agency, 2026g]; [Union, 2024]; [of Europe, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

70.2.2.1 Lesson 1: Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks

Concept. Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks focuses on transparent resilience education: provenance, audience harm, attribution caution, and non-manipulative response options.

Why it matters. Without explicit treatment of **Intelligence Ethics**, treating resilience labels as permission to skip provenance review undermines authority mapping and rights-aware release review; the lesson builds the habit to separate having a capability from having authority and accountable review.

Source support. Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks rests on [298, 2026] and [297, 2026]. Its anchor reference records: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for the claim that **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Archives and Administration, 1981]; [Agency, 2026g].

Evidence to inspect. Ground **Intelligence Ethics** in the evidence the row cites. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Intelligence Ethics**, build a **authority-and-impact register with approvals, limits, public notice, audit owners, and review dates** for this authority mapping and rights-aware release review topic. The artifact must record the narrative provenance, the bounded claim about **Intelligence Ethics**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Intelligence Ethics** work as an **authority-and-impact review register** that logs the evidence, the uncertainty, the responsible reviewer, and the halt condition.

Misconception check. Correct the misconception about **Intelligence Ethics**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **Intelligence Ethics** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

70.2.2.2 Lesson 2: The Ethics of Cognitive Security (YorkSpace Dissertation)

Concept. The Ethics of Cognitive Security (YorkSpace Dissertation) maps cognitive attack surfaces: attention, belief formation, narrative provenance, and transparent correction options.

Why it matters. The Ethics of Cognitive Security (YorkSpace Dissertation) connects classroom vocabulary to Legal, Ethical, and Oversight Architecture practice: learners document evidence, caveats, and reviewer ownership rather than repeating labels.

Source support. The Ethics of Cognitive Security (YorkSpace Dissertation) rests on [172, 2026]. The lead source's own note reads: This 2023 York University doctoral dissertation by Andrew Ward Buzzell provides an ethical and epistemic assessment of state power exercised to defend against information threats, a domain the author terms cognitive security. Use it for the claim that **The Ethics of Cognitive Security (YorkSpace Dissertation)** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Archives and Administration, 1981]; [Agency, 2026g].

Evidence to inspect. Read **The Ethics of Cognitive Security (YorkSpace Dissertation)** against the works cited for this row. [172, 2026] This 2023 York University doctoral dissertation by Andrew Ward Buzzell provides an ethical and epistemic assessment of state power exercised to defend against information threats, a domain the author terms cognitive security. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **The Ethics of Cognitive Security (YorkSpace Dissertation)**, build a **authority-and-impact register with approvals, limits, public notice, audit owners, and review dates** for this authority mapping and rights-aware release review topic. The artifact must record the narrative provenance, the bounded claim about **Ethics of Cognitive Security**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape this subject work as an **authority-and-impact review register** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **The Ethics of Cognitive Security (YorkSpace Dissertation)**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **The Ethics of Cognitive Security (YorkSpace Dissertation)** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

70.2.2.3 Lesson 3: AI Ethics in Intelligence: Accountability, Transparency, Proportionality

Concept. AI Ethics in Intelligence: Accountability, Transparency, Proportionality — Test whether a method is no more intrusive than the accountable need justifies and whether affected groups have redress.

Why it matters. AI Ethics in Intelligence matters in the **Legal, Ethical, and Oversight Architecture** lane because authority mapping and rights-aware release evidence must stay separate from judgment; treating resilience labels as permission to skip provenance review is a common failure.

Source support. AI Ethics in Intelligence: Accountability, Transparency, Proportionality rests on [298, 2026] and [297, 2026]. The most specific cited work observes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for pinning down the scope of **AI Ethics in Intelligence: Accountability, Transparency, Proportionality**, the edge of that scope, and when these citations need re-verifying before transfer. External triangulation uses [Archives and Administration, 1981]; [Agency, 2026g].

Evidence to inspect. For **AI Ethics in Intelligence**, work from the cited evidence behind this row. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Read each cited work for what it can support about this topic, where that claim originated, how confident it is, and what evidence would change it.

Student artifact. For **AI Ethics in Intelligence**, build a **authority-and-impact register with approvals, limits, public notice, audit owners, and review dates** for this authority mapping and rights-aware release review topic. The artifact must record the narrative provenance, the bounded claim about **AI Ethics in Intelligence**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **AI Ethics in Intelligence** work as an **authority-and-impact review register** that names evidence, uncertainty, reviewer, and stop condition.

Misconception check. Correct the misconception about **AI Ethics in Intelligence**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Reuse the **AI Ethics in Intelligence** audit pattern from this module on a different sample record set with a new reviewer and blocked-use note.

70.2.2.4 Lesson 4: Oversight Mechanisms: Congressional, Inspector General, FISA Court

Concept. Oversight Mechanisms: Congressional, Inspector General, FISA Court maps the legal source to authority, oversight, retention, and redress fields before any workflow is allowed.

Why it matters. Analysts use **Oversight Mechanisms** to separate having a capability from having authority and accountable review. A defensible treatment names the judgment it enables for authority mapping and rights-aware release review, the proof limit that treating resilience labels as permission to skip provenance review would otherwise hide, and the reviewer accountable for challenge.

Source support. Oversight Mechanisms: Congressional, Inspector General, FISA Court rests on [298, 2026] and [297, 2026]. The closest source to this row notes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for the working definition that **Oversight Mechanisms: Congressional, Inspector General, FISA Court** can defend, where that scope ends, and the refresh check owed before this evidence transfers. External triangulation uses [Archives and Administration, 1981]; [Agency, 2026g].

Evidence to inspect. Read **Oversight Mechanisms** against the works cited for this row. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Work source by source: name the bounded claim, its origin, the residual uncertainty, and the trigger that would change how this topic is judged.

Student artifact. For **Oversight Mechanisms**, build a **authority-and-impact register with approvals, limits, public notice, audit owners, and review dates** for this authority mapping and rights-aware release review topic. The artifact must record the narrative provenance, the bounded claim about **Oversight Mechanisms**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape **Oversight Mechanisms** work as an **authority-and-impact review register** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Oversight Mechanisms**: that a legal source grants authority without scope and oversight.

Transfer task. Apply this module's safe boundary for **Oversight Mechanisms** to another artifact while keeping authority mapping and rights-aware release review and reviewer ownership explicit.

70.2.2.5 Lesson 5: Whistleblowing, Leaking, and the Epistemic Duty of Intelligence Professionals

Concept. Whistleblowing, Leaking, and the Epistemic Duty of Intelligence Professionals — Separate lawful disclosure channels, source protection, and oversight from unauthorized release or targeting narratives.

Why it matters. Without explicit treatment of **Whistleblowing, Leaking, and the Epistemic Duty of Intelligence Professionals**, treating resilience labels as permission to skip provenance review undermines authority mapping and rights-aware release review; the lesson builds the habit to separate having a capability from having authority and accountable review.

Source support. Whistleblowing, Leaking, and the Epistemic Duty of Intelligence Professionals rests on [298, 2026] and [297, 2026]. The most specific cited work observes: Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. Use them for the claim that **Whistleblowing, Leaking, and the Epistemic Duty of Intelligence Professionals** lets you defend here, the limit it has to respect, and the re-check owed before reuse. External triangulation uses [Archives and Administration, 1981]; [Agency, 2026g].

Evidence to inspect. Read **Whistleblowing, Leaking, and the Epistemic Duty of Intelligence Professionals** against the works cited for this row. [298, 2026] Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations. [297, 2026] Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products. From each source, pull the bounded claim it can carry for this topic, its provenance, the stated uncertainty, and the one condition that would overturn that judgment.

Student artifact. For **Whistleblowing, Leaking, and the Epistemic Duty of Intelligence Professionals**, build a **authority-and-impact register with approvals, limits, public notice, audit owners, and review dates** for this authority mapping and rights-aware release review topic. The artifact must record the narrative provenance, the bounded claim about **Whistleblowing Leaking and the Epistemic**, the audience-harm caveat, the uncertainty note, the transparent-use boundary, and the reviewer accountable for correction. Shape this subject work as an **authority-and-impact review register** that states the evidence used, what stays uncertain, who reviews it, and when to stop.

Misconception check. Correct the misconception about **Whistleblowing, Leaking, and the Epistemic Duty of Intelligence Professionals**: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

Transfer task. Transfer **Whistleblowing, Leaking, and the Epistemic Duty of Intelligence Professionals** from this module to a second motif by preserving authority mapping and rights-aware release review, replacing action with audit, and naming the blocked use.

70.2.3 Ethics of Intelligence and Cognitive Security worked safe example: synthetic inputs, evidence, and review

Worked example: a sample agency training team reviews whether a classroom AI workflow is allowed. [238, 2026]; [239, 2026].

Triangulation anchors. In module 51's worked-example section, directly verified anchors for the **Legal, Ethical, and Oversight Architecture** lane include [Archives and Administration, 1981]; [Agency, 2026g]; [Union, 2024]; [of Europe, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Unit discipline spine. Discipline: **authority, rights, oversight, and auditability**. Learners use a **authority-and-impact review register** and keep this boundary visible: Capability never substitutes for legal authority, accountable review, affected-person safeguards, or auditability.

Frame. The classroom question centers on **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks**. Excluded actions stay explicit, and the **Oversight-and-Rights Lens** planning question is: Which authority, impact assessment, public-register entry, audit record, and escalation path must exist before the workflow is allowed?

Inputs. For the **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks** scenario, use public policy excerpts, synthetic workflow notes, a rights-impact checklist, and an audit-log template. The Oversight-and-Rights Lens intake note records provenance, sensitivity,

fit-to-purpose, and why the fixture is enough for this bounded exercise.

Analysis. For **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks**, students map authority, test proportionality, name affected groups, assign oversight, and define redress or escalation. Pause whenever an inference about Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks appears without evidence, confidence outruns support, or an agent output is treated as judgment.

Filled artifact. Purpose = **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks** classroom scenario; unit artifact = authority-and-impact review register; evidence = allowed inputs; method = authority mapping and rights-aware release review; output = an authority-and-impact register with approvals, limits, audit owner, and review date; boundary = no external action; reviewer = instructor or named peer.

Flawed answer to revise. Treating **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks** as "Oversight-and-Rights Lens confirms it" is not enough. The revision ties the claim to authority mapping and rights-aware release review, adds the missing caveat, states confidence, and records the reviewer who accepted the bounded judgment.

Debrief. The reuse note for **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks** records the defensible claim, the assumption most likely to fail, the evidence that would change confidence, and the review condition for stopping reuse.

70.2.4 Ethics of Intelligence and Cognitive Security practice sequence: studio moves, artifact steps, and limits

The studio sequence uses the **Oversight-and-Rights Lens** practice lens. Moves 1-3 form the compressed path; the full seminar path adds challenge, handoff, and a review memo for **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security**.

Triangulation anchors. In module 51's practice-sequence section, directly verified anchors for the **Legal, Ethical, and Oversight Architecture** lane include [Archives and Administration, 1981]; [Agency, 2026g]; [Union, 2024]; [of Europe, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Move	Learner action	Output	Check
1. Distinguish	Compare Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks, The Ethics of Cognitive Security, AI Ethics in Intelligence: Accountability, Transparency, Proportionality; name what each topic can and cannot prove.	Glossary-and-contrast card.	Terms match the **Legal, Ethical, and Oversight Architecture** lane.
2. Frame	Answer the lens question: Which authority, impact assessment, public-register entry, audit record, and escalation path must exist before the workflow is allowed?	Scope card.	Authority, excluded actions, data boundary, and reviewer are explicit.
3. Evidence	Fill the artifact fields for Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks: authority-and-impact register with approvals, limits, public notice, audit owners, and review dates.	Evidence packet.	Sources, caveats, confidence, and uncertainty stay separable.
3a. Unit artifact	Add the authority-and-impact review register fields for Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks.	Unit profile note.	Evidence artifacts include authority map, rights-impact note.
4. Challenge	Test the misconception that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.	Failure-mode note.	The artifact applies the key distinction: separate having a capability from having authority and accountable review.
5. Handoff	Prepare the artifact for another reviewer.	Handoff memo.	Inputs, transformations, reviewer, refresh trigger, and residual risk are visible.

70.2.4.1 Ethics of Intelligence and Cognitive Security instructor notes: source reasoning, review points, and studio focus

Ask learners to verbalize the difference between a source, an inference, and a decision. Require a revision whenever a claim cannot be traced to a source descriptor or a human review point. Keep the focus on **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security**. [238, 2026]; [239, 2026].

70.2.4.2 Ethics of Intelligence and Cognitive Security extension exercise: peer validation and refresh trigger review

Evidence anchor. Section 70; [238, 2026].

Have learners swap artifacts and apply the **Oversight-and-Rights Lens** validation rule to someone else's work. The receiving learner must identify one strength, one missing caveat, and one refresh trigger for **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security**.

70.2.5 Ethics of Intelligence and Cognitive Security knowledge check: misconceptions, evidence, and reviewer prompts

Evidence anchor. Section 70; [238, 2026].

1. Explain how **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks** is defined here; name the source descriptor that supports the definition.
2. Contrast **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks** with **The Ethics of Cognitive Security** using the **Oversight-and-Rights Lens** artifact fields.
3. Identify one failure mode from the **Legal, Ethical, and Oversight Architecture** lane and the evidence that would reveal it.
4. Answer the coursebook review question: What control turns a capability into an accountable, reviewable workflow?

5. Correct this misconception: that a resilience label on a technique means it has been stress-tested, rather than a habit that still needs evidence, caveats, and reviewer challenge.

70.2.5.1 Ethics of Intelligence and Cognitive Security answer quality rubric: source evidence, uncertainty, and safe transfer Judge answers with the canonical mastery evidence standard in the shared method-and-assurance reference (Section 3): a strong answer uses source evidence, distinguishes observation from judgment, names uncertainty, and states the safe boundary, while a revise-level answer gives a memorized definition of **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks** without source evidence, uncertainty, or a safe transfer task.

70.3 Ethics of Intelligence and Cognitive Security assurance handoff: evidence, governance, refresh, and capstone

Evidence anchor. Section 70; [238, 2026].

70.3.1 Ethics of Intelligence and Cognitive Security evidence contract: source spine, verified anchors, transfer architecture, and claim limits

Evidence anchor. Section 70; [238, 2026].

70.3.2 Ethics of Intelligence and Cognitive Security transfer architecture: module inputs, outputs, and review boundary

Evidence anchor. Section 70; [238, 2026].

70.3.2.1 Ethics of Intelligence and Cognitive Security lineage and source tradition: profile, concepts, and first anchors This sits in the **Legal, Ethical, and Oversight Architecture** lineage: turning authority, accountability, transparency, and review into design constraints rather than post-hoc paperwork. [238, 2026]; [239, 2026].

70.3.2.2 Ethics of Intelligence and Cognitive Security working model: inputs, constraints, transforms, outputs, and oversight **Evidence anchor.** Section 70; [238, 2026].

The work is modeled as inputs, constraints, transforms, outputs, feedback, and oversight for **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security**, with provenance and reviewability throughout.

70.3.2.3 Ethics of Intelligence and Cognitive Security knowledge architecture: inputs, transforms, outputs, and failure checks

- **Inputs:** legal authorities, policy constraints, affected groups, retention duties, oversight roles, and audit logs. [238, 2026]; [239, 2026].
- **Transforms:** authority mapping, proportionality review, rights-impact assessment, redress planning, and escalation routing.
- **Outputs:** authority-and-impact register, audit trail, redress note, and unresolved-risk owner.
- **Failure modes:** authority laundering, missing audit trails, privacy overreach, and governance-as-afterthought.

70.3.2.4 Ethics of Intelligence and Cognitive Security transfer contracts: authority, evidence, tools, and auditable output **Evidence anchor.** Section 70; [238, 2026].

- **Authority contract:** define why the work is being practiced, who reviews it, and which actions are excluded for **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security**.
- **Evidence contract:** keep the **Legal, Ethical, and Oversight Architecture** source descriptors, transformations, claims, uncertainty, and confidence separable.
- **Tool contract:** bind any agent assistance to explicit tools, permissions, budgets, logging, and rollback conditions.
- **Output contract:** render the chapter artifact as authority-and-impact register, audit trail, redress note, and unresolved-risk owner that another reviewer can audit.

70.3.2.5 Ethics of Intelligence and Cognitive Security profile emphasis and local focus: method stack and topic cluster **Evidence anchor.** Section 70; [238, 2026].

The matched profile emphasizes turning authority, accountability, transparency, and review into design constraints rather than post-hoc paperwork. The method stack is authority mapping, role assignment, impact assessment, documentation review, escalation triggers, and independent oversight; the local topic cluster is **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security**.

70.3.3 Ethics of Intelligence and Cognitive Security evidence spine: source roles, citation support, and claim limits

Evidence anchor. Section 70; [238, 2026].

Guide citations preserve the inherited bibliography, verified anchors supply lane constraints, and the **Legal, Ethical, and Oversight Architecture** profile tells reviewers what evidence is strong enough for the module artifact built around **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security**.

70.3.3.1 Ethics of Intelligence and Cognitive Security guide source spine: inherited keys and local citation roles Primary guide citations: [238, 2026]; [239, 2026]; [240, 2026]; [278, 2026]; [279, 2026]; [283, 2026]; [290, 2026]; [291, 2026]; [294, 2026]; [172, 2026]; [298, 2026]; [297, 2026].

70.3.3.2 Ethics of Intelligence and Cognitive Security verified source canon: direct anchors and claim boundaries The source canon has three tiers; the local spine begins with [238, 2026]; [239, 2026].

Tier	What counts	How it is used
Source guide	[238, 2026]; [239, 2026]; [240, 2026]; [278, 2026]; [279, 2026]; [283, 2026]; [290, 2026]; [291, 2026]; [294, 2026]; [172, 2026]; [298, 2026]; [297, 2026].	Preserves the inherited AGEINT outline and `ageintNNN` keys.
Verified anchors	Official, standards, public-domain, or scholarly sources in `references-*.bib`	Supplies governance, quality, legal, safety, and technical constraints.
Runtime profile	The profile matched to the current unit and current module	Selects the practice lens, method stack, failure modes, and defensive boundary for generated prose.

Triangulation anchors. In module 51's source-canon section, directly verified anchors for the **Legal, Ethical, and Oversight Architecture** lane include [Archives and Administration, 1981]; [Agency, 2026g]; [Union, 2024]; [of Europe, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Maintenance rule: Perplexity may suggest candidates for **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security** and [238, 2026]; [239, 2026], but only directly verified source URLs are encoded as citations.

70.3.3.3 Ethics of Intelligence and Cognitive Security intelligence practice lens: evidence artifact and safety check Practice lens: **Oversight-and-Rights Lens** for **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security**. [238, 2026]; [239, 2026].

Planning question: Which authority, impact assessment, public-register entry, audit record, and escalation path must exist before the workflow is allowed?

Evidence artifact: authority-and-impact register with approvals, limits, public notice, audit owners, and review dates.

Validation rule: confirm lawful purpose, proportionality, retention, review, and appeal or redress paths. Applied to **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security**.

Handoff contract: handoff includes approvals, policy constraints, audit evidence, and unresolved legal or ethical issues.

Safety check: reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought.

70.3.3.4 Ethics of Intelligence and Cognitive Security runtime-to-reader map: generated sections and verifier surfaces Evidence anchor. Section 70; [238, 2026].

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
Source-lane evidence, public registers, and claim-ledger studio	51.99	51.99 source title transformed into safe curriculum treatment; original: V2 source-lane extension: bind Ethics of Intelligence and Cognitive Security to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
Bounded autonomy, procurement, incident-response, and assurance studio	51.101	51.101 source title transformed into safe curriculum treatment; original: Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Ethics of Intelligence and Cognitive Security	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
Model-card, recoverability, retention, and learner-support evidence package	51.102	51.102 source title transformed into safe curriculum treatment; original: Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Ethics of Intelligence and Cognitive Security	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks	51.1	51.1 Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought

Rendered title	Source loci	Source provenance	Practice lens	Evidence artifact	Safety check
The Ethics of Cognitive Security (YorkSpace Dissertation)	51.2	51.2 The Ethics of Cognitive Security (YorkSpace Dissertation)	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
AI Ethics in Intelligence: Accountability, Transparency, Proportionality	51.3	51.3 AI Ethics in Intelligence: Accountability, Transparency, Proportionality	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
Oversight Mechanisms: Congressional, Inspector General, FISA Court	51.4	51.4 Oversight Mechanisms: Congressional, Inspector General, FISA Court	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
Whistleblowing, Leaking, and the Epistemic Duty of Intelligence Professionals	51.5	51.5 Whistleblowing, Leaking, and the Epistemic Duty of Intelligence Professionals	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought

70.3.3.5 Ethics of Intelligence and Cognitive Security reusable subsection contract: topic rows, artifacts, and safety duties Evidence anchor. Section 70; [238, 2026].

Lesson topic	Practice lens	Evidence artifact	Safety check
Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
The Ethics of Cognitive Security (YorkSpace Dissertation)	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
AI Ethics in Intelligence: Accountability, Transparency, Proportionality	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
Oversight Mechanisms: Congressional, Inspector General, FISA Court	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought
Whistleblowing, Leaking, and the Epistemic Duty of Intelligence Professionals	Oversight-and-Rights Lens	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates	reject authority laundering, privacy overreach, unmanaged retention, and governance-as-afterthought

70.3.3.6 Ethics of Intelligence and Cognitive Security annotated source ledger: real titles and local contribution Each source cited by this **Legal, Ethical, and Oversight Architecture** module is paired below with its real title and a one-line note on what it contributes to **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security**.

Source	Cited work	What it contributes	Status
[238, 2026]	Recommendation on the Ethics of Artificial Intelligence	The official UNESCO page for the Recommendation on the Ethics of Artificial Intelligence, the first global standard-setting instrument on AI ethics, adopted in 2021 and applicable to all 194 member states. It outlines four core values, including human rights protection and environmental flourishing, and ten guiding principles such as proportionality, privacy, transparency, and fairness.	verified source-guide
[239, 2026]	Digital Space and Human Rights	Official OHCHR digital rights portal.	original source-guide

Source	Cited work	What it contributes	Status
[240, 2026]	The Right to Privacy in the Digital Age	The Office of the High Commissioner for Human Rights (OHCHR) hub page on the right to privacy in the digital age. It addresses how data-intensive technologies, particularly artificial intelligence, create risks for privacy, autonomy, and human dignity, and curates international standards, reports, and expert consultations.	verified source-guide
[278, 2026]	Recommendation of the Council on Public Procurement	The OECD Recommendation of the Council on Public Procurement (OECD/LEGAL/0411), a legal instrument adopted by the OECD Council in 2015 on the proposal of the Public Governance Committee. It frames public procurement as a pillar of strategic governance and service delivery and sets out principles for governments to follow.	verified source-guide
[279, 2026]	Open Contracting Data Standard	The documentation homepage for the Open Contracting Data Standard, version 1.1.5, maintained by the Open Contracting Partnership to support disclosure of government contracting data across the procurement lifecycle. It provides a common data model spanning planning, tender, award, contract, and implementation stages, along with a primer, implementation guidance, technical schemas, and validation tooling.	verified source-guide
[283, 2026]	Recommendation of the Council on Open Government	An OECD legal instrument document reproducing the Recommendation of the Council on Open Government (OECD/LEGAL/0438), adopted on 14 December 2017. It defines open government as a culture of governance promoting transparency, integrity, accountability, and stakeholder participation in support of democracy and inclusive growth.	verified source-guide
[290, 2026]	NIST SP 800-218A: Secure Software Development Practices for Generative AI and Dual-Use Foundation Models	NIST Special Publication 800-218A (July 2024), which augments the Secure Software Development Framework with practices specific to AI model development across the software lifecycle. Produced in response to Executive Order 14110, it addresses AI model producers, developers building on those models, and acquirers of AI systems, and is designed to be used alongside NIST SP 800-218.	verified source-guide
[291, 2026]	Revised 508 Standards and 255 Guidelines	Official documentation from the U.S. Access Board on the Revised 508 Standards and 255 Guidelines for information and communication technology accessibility. It establishes mandatory accessibility requirements for federal agencies and voluntary guidelines for telecommunications manufacturers, covering hardware, software, websites, electronic documents, and support services.	verified source-guide

Source	Cited work	What it contributes	Status
[294, 2026]	M-25-21: Accelerating Federal Use of AI through Innovation, Governance, and Public Trust	An April 2025 Office of Management and Budget memorandum (M-25-21) directing executive branch agencies on federal use of artificial intelligence. Issued under Executive Order 14179, it instructs agencies to accelerate adoption of AI to improve public services and government efficiency while maintaining safeguards for civil rights, civil liberties, and privacy.	verified source-guide
[172, 2026]	The Ethics of Cognitive Security - YorkSpace	This 2023 York University doctoral dissertation by Andrew Ward Buzzell provides an ethical and epistemic assessment of state power exercised to defend against information threats, a domain the author terms cognitive security.	verified source-guide
[298, 2026]	Intelligence Community Directives	Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations.	original source-guide
[297, 2026]	Intelligence Community Directive 203: Analytic Standards	Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products.	original source-guide

Where this sits. This module's overview is Section 70; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

70.3.4 Ethics of Intelligence and Cognitive Security governance boundary: synthesis, agent-assistance rules, rights, and assurance gates

Evidence anchor. Section 70; [238, 2026].

70.3.5 Ethics of Intelligence and Cognitive Security analytic synthesis: source-backed claims and forbidden leaps

Triangulation anchors. In module 51's governance-boundary section, directly verified anchors for the **Legal, Ethical, and Oversight Architecture** lane include [Archives and Administration, 1981]; [Agency, 2026g]; [Union, 2024]; [of Europe, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

Research lane: **Legal, Ethical, and Oversight Architecture** for **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security (YorkSpace Dissertation)**. [238, 2026]; [239, 2026].

Curriculum topic spine: Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks, **The Ethics of Cognitive Security (YorkSpace Dissertation)**, **AI Ethics in Intelligence: Accountability, Transparency, Proportionality**. **Verified anchor cluster:** [Archives and Administration, 1981]; [Agency, 2026g]; [Union, 2024]; [of Europe, 2024]; [Privacy and Board, 2026]; [Community, 2020b]; [Community, 2020a].

Conceptual depth: turning authority, accountability, transparency, and review into design constraints rather than post-hoc paperwork.

Method stack: authority mapping, role assignment, impact assessment, documentation review, escalation triggers, and independent oversight.

Composability contract: policies, approvals, audit logs, evidence, and action permissions remain linked but independently inspectable.

Known failure modes: authority laundering through tools, missing audit trails, privacy overreach, and treating governance as a static checklist.

Defensive boundary: governance content supports lawful design, education, and review; it does not justify unauthorized collection or deployment. Applied to **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security (YorkSpace Dissertation)**.

Anchor	Why it matters here
[Archives and Administration, 1981]	Official legal anchor for intelligence authorities, rights-aware collection, analytic competition, oversight, and source-method protection. Checked as of 2026-05-21; role: curriculum_anchor.
[Agency, 2026g]	Official NSA public explanation of FISA oversight for signals intelligence collection governed by statutory and court-authorized controls. Checked as of 2026-05-21; role: curriculum_anchor.
[Union, 2024]	Official EU Artificial Intelligence Act legal text. Checked as of 2026-05-21; role: source_quality_anchor.
[of Europe, 2024]	Official treaty anchor for human rights, democracy, rule-of-law, risk management, accountability, and public-sector AI governance. Checked as of 2026-05-21; role: curriculum_anchor.
[Privacy and Board, 2026]	Official oversight-report library for privacy, civil-liberties, surveillance, watchlisting, facial-recognition, and redress analysis. Checked as of 2026-05-21; role: curriculum_anchor.
[Community, 2020b]	Official IC principles for lawful, accountable, objective, human-centered, secure, resilient, and science-informed AI. Checked as of 2026-05-21; role: curriculum_anchor.
[Community, 2020a]	Official IC framework for AI goals, authorities, human judgment, bias mitigation, testing, documentation, explainability, and review. Checked as of 2026-05-21; role: curriculum_anchor.

70.3.5.1 Ethics of Intelligence and Cognitive Security evidence standard and citation floor: source families and discovery limits

Official guidance supplies governance, safety, and legal constraints for the **Legal, Ethical, and Oversight Architecture** lane; scholarly or policy-scholarship sources supply explanatory frames; source-guide citations preserve the inherited AGEINT bibliography. Perplexity-assisted discovery is allowed during maintenance, but the manuscript citation itself must resolve to a direct source URL in `references-*.bib`. Local checks start with [238, 2026]; [239, 2026].

70.3.6 Ethics of Intelligence and Cognitive Security agentic boundary: assist, approve, block, and record

Evidence anchor. Section 70; [238, 2026].

AGEINT translation is bounded by the **Legal, Ethical, and Oversight Architecture** lane. Agents may organize sources, retrieve context, compare alternatives, draft checklists, summarize evidence, simulate benign scenarios, and audit reasoning. They do not initiate unauthorized collection, exploitation, covert targeting, manipulation, or cyber-physical action; examples stay tied to **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security**.

70.3.6.1 Ethics of Intelligence and Cognitive Security permitted defensive utility: curriculum uses and safe outputs **Evidence anchor.** Section 70; [238, 2026].

The defensive utility is curriculum design, tabletop preparation, risk assessment, governance review, source evaluation, and resilience planning. Work products fit the current unit's education, policy review, lab exercises, and accountable defensive analysis for **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security**.

70.3.6.2 Ethics of Intelligence and Cognitive Security excluded operational boundary: blocked actions and stop rules

Keep all practice accountable, synthetic, defensive, logged, reversible, and evidence-bounded while working from [238, 2026]; [239, 2026] and **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security**. Do not convert it into live targeting, evasion, exploitation, covert collection, manipulation, or unsafe cyber-physical action.

70.3.7 Ethics of Intelligence and Cognitive Security governance assurance: authority, rights, evidence, and human review

Evidence anchor. Section 70; [238, 2026].

Governance is practiced as a gate on the **Legal, Ethical, and Oversight Architecture** lane. Learners use the **Oversight-and-Rights Lens** to decide who is accountable for the exercise, which evidence is sufficient, what rights and access issues remain, and when an agent-assisted artifact must stop for human review while using **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security**.

70.3.7.1 Ethics of Intelligence and Cognitive Security governance card: gates, retained evidence, and review owner

Gate	Coursebook check	Evidence retained
Authority	The exercise has a lawful, educational, or defensive purpose and named reviewer.	scope card, excluded-action list, and reviewer initials
Evidence	Claims in this module remain tied to guide citations or verified anchors starting with [238, 2026]; [239, 2026].	claim ledger, source descriptors, caveats, and confidence language
Rights and access	Privacy, accessibility, learner support, and affected-group impacts are considered before reuse.	rights note, accommodation path, and unresolved-risk owner
Agent control	Any agent assistance stays bounded to retrieval, comparison, drafting, simulation, critique, or audit.	tool allowlist, prompt/output record, stop condition, and rollback note
Assurance	The artifact is challenged against **Legal, Ethical, and Oversight Architecture** failure modes and the **Oversight-and-Rights Lens** safety check.	failure-mode note, remediation item, retest result, and refresh trigger

70.3.7.2 Ethics of Intelligence and Cognitive Security evidence package handoff: appendices, records, and reuse **Evidence anchor.** Section 70; [238, 2026].

Detailed model/data cards, transparency notices, retention rows, release gates, risk exceptions, incident drills, procurement checks, and learner-support workflows live in the generated appendices and source-support docs. The local **Oversight-and-Rights Lens** evidence gate stays compact enough to apply during reading, practice, and revision for **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security**.

70.3.7.3 Ethics of Intelligence and Cognitive Security current-source assurance: verified anchors and local artifact fit The source assurance check ties the current verified anchor set to the local chapter artifact instead of relying on discovery summaries, here covering **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security**. [238, 2026]; [239, 2026].

Assurance question	Direct source evidence	Chapter artifact
What does the module inherit from `official_odni_eo_12333` for **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security**?	Executive Order 12333: United States Intelligence Activities; lane `legal_oversight`; checked 2026-05-21.	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates; Official legal anchor for intelligence authorities, rights-aware collection, analytic competition, oversight, and source-method protection.
What does the module inherit from `official_nsa_fisa` for **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security**?	Foreign Intelligence Surveillance Act; lane `legal_oversight`; checked 2026-05-21.	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates; Official NSA public explanation of FISA oversight for signals intelligence collection governed by statutory and court-authorized controls.
What does the module inherit from `official_eu_ai_act` for **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security**?	Regulation (EU) 2024/1689: Artificial Intelligence Act; lane `source_quality_spine`; checked 2026-05-21.	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates; Official EU Artificial Intelligence Act legal text.
What does the module inherit from `official_council_europe_ai_convention` for **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security**?	Framework Convention on Artificial Intelligence; lane `legal_oversight`; checked 2026-05-21.	authority-and-impact register with approvals, limits, public notice, audit owners, and review dates; Official treaty anchor for human rights, democracy, rule-of-law, risk management, accountability, and public-sector AI governance.
How is Perplexity handled here?	Discovery and second-opinion notes are not citable authority unless converted into direct official, standards-body, public-domain, or scholarly anchors.	Claim ledger records the direct URL, checked date, source lane, refresh trigger, and reviewer.

Where this sits. This module's overview is Section 70; return to the curriculum atlas Section 2 for the reader paths, evidence map, and safety gates that govern this module.

70.3.8 Ethics of Intelligence and Cognitive Security assessment route: capstone artifacts, refresh duties, reviewer challenges, and handoff

Evidence anchor. Section 70; [238, 2026].

70.3.9 Ethics of Intelligence and Cognitive Security assessment pathway: capstone artifacts and mastery evidence

Evidence anchor. Section 70; [238, 2026].

70.3.9.1 Ethics of Intelligence and Cognitive Security capstone pathway: reviewable packet and excluded use The capstone deliverable is a reviewable packet that plugs into the broader unit thread. Run it through the canonical phase, artifact, and review-gate ladder in the shared method-and-assurance reference (Section 3); the local topic cluster is **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security**.
Minimum module submission: one-page analytic memo, source-lane map, claim ledger, safe-lab packet, rubric self-assessment, and debrief note. The packet must name what is excluded, who may approve reuse, and what would trigger a source refresh for **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security** and [238, 2026]; [239, 2026].

70.3.9.2 Ethics of Intelligence and Cognitive Security instructor facilitation notes: studio roles and pause points Facilitate as a bounded studio around **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security**, not as a lecture-only session.

- Start with the authority card and excluded-action list before showing examples from **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security** and [238, 2026]; [239, 2026].
- Assign one learner to maintain the claim ledger and one learner to challenge source quality.
- Keep agent prompts visible enough for review and separate from final judgment.
- Pause any activity that drifts toward live systems, real people, sensitive data, or external action.
- End with a debrief that separates evidence learned, uncertainty preserved, rights impact, and next refresh owner.

70.3.9.3 Ethics of Intelligence and Cognitive Security assessment rubric: topic evidence and mastery criteria

Topic	Evidence of mastery
Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks	Completed **authority-and-impact register with approvals, limits, public notice, audit owners, and review dates** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
The Ethics of Cognitive Security (YorkSpace Dissertation)	Completed **authority-and-impact register with approvals, limits, public notice, audit owners, and review dates** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.
AI Ethics in Intelligence: Accountability, Transparency, Proportionality	Completed **authority-and-impact register with approvals, limits, public notice, audit owners, and review dates** with source descriptor, caveat, uncertainty, blocked-use note, and named reviewer for this topic.

The general competency and mastery rubric is the canonical five-row rubric in the shared method-and-assurance reference (Section 3), covering conceptual command, analytic rigor, agentic design, governance and rights, and safety posture. Score the artifact for **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security** against that rubric together with the topic-specific evidence rows above so conceptual command, uncertainty handling, oversight design, rights evidence, and evidence-bounded posture stay visible.

70.3.10 Ethics of Intelligence and Cognitive Security refresh map: source changes, safety triggers, and retest duties

Source changes, unsafe wording, inaccessible artifacts, rights triggers, tool incidents, and instructor debrief findings each produce a visible owner, action, and retest condition before the module is reused against [238, 2026]; [239, 2026] and **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security**.

70.3.10.1 Ethics of Intelligence and Cognitive Security refresh triggers: source changes and required actions Refresh against the canonical trigger-and-action table in the shared method-and-assurance reference (Section 3). When a source-guide reference, official standard, AI or public-sector policy, interface specification, safety audit, or instructor debrief signal appears, take the matching required action before reuse for **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security**. The local signals begin with [238, 2026]; [239, 2026].

70.3.10.2 Ethics of Intelligence and Cognitive Security claim and evidence ledger: claim classes, caveats, and owners The claim and evidence ledger follows the canonical claim-class ladder in the shared method-and-assurance reference (Section 3). Apply the source-spine, research-backed governance, agentic-workflow, empirical or evaluated capability, safety, and cross-module claim classes to every assertion, attaching the required evidence and clearing the matching review gate before reuse. The local topic cluster is **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security**, and the source spine for these checks begins with [238, 2026]; [239, 2026].

70.3.11 Ethics of Intelligence and Cognitive Security reviewer challenge route: checklist, failure evidence, and remediation

Before marking the work complete, verify the local source spine beginning with [238, 2026]; [239, 2026].
Triangulation anchors. In module 51's review-checklist section, directly verified anchors for the **Legal, Ethical, and Oversight Architecture** lane include [Archives and Administration, 1981]; [Agency, 2026g]; [Union, 2024]; [of Europe, 2024]. Use them to test source-guide claims, method boundaries, governance constraints, and safety gates without replacing the module's `ageintNNN` provenance.

- The module source spine resolves to Pandoc citation keys and no raw source URLs are pasted into prose, here covering **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security**. [238, 2026]; [239, 2026].
- Every research-backed claim has a directly verified source anchor or is clearly marked as source-guide context.
- Agentic affordances are limited to retrieval, comparison, drafting, simulation, critique, and audit support.
- The lab packet uses public, benign, owned-lab, or synthetic material only.
- The artifact names assumptions, caveats, uncertainty, excluded actions, and human review points.
- No Figure, Section, Equation, chapter, or appendix numbers are hard-coded outside generated labels.

70.3.12 Ethics of Intelligence and Cognitive Security learning-path links: module map, overview, and curriculum atlas

Follow the cross-links to move between **Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks; The Ethics of Cognitive Security** and the rest of the curriculum without losing the source spine: orientation first, then the parent unit, then the modules on either side. Primary sources: [238, 2026]; [239, 2026].

Section 2, Section 68, Section 69, Section 71

71 Python OSINT Library

The current appendix is an evidence workbook for reusable classroom methods. It is educational and evidence-bounded: examples remain synthetic, defensive, lawful, and bounded to owned labs, public sources, or tabletop exercises. Source-item focus: Recon-ng Module Development: Custom Data Source Integration; SpiderFoot Custom Module: Target Intelligence Aggregation.

71.1 Python OSINT Library workbook scope: purpose, safety envelope, and reuse decision

Section anchor. Section 71.

71.1.1 Python OSINT Library operating purpose

Section anchor. Section 71.

The current appendix supports a reusable methods workbook. Each source item is treated as a reviewable classroom artifact rather than an operational instruction; examples begin with Recon-ng Module Development: Custom Data Source Integration; SpiderFoot Custom Module: Target Intelligence Aggregation.

71.1.2 Python OSINT Library allowed-input boundary

Section anchor. Section 71.

Allowed inputs for the current appendix are public official or scholarly sources, standards text, instructor-provided excerpts, synthetic datasets, owned-lab logs, toy examples, and generated rubrics that expose their provenance for Recon-ng Module Development: Custom Data Source Integration; SpiderFoot Custom Module: Target Intelligence Aggregation.

71.1.3 Python OSINT Library excluded-action boundary

Section anchor. Section 71.

Excluded actions for the current appendix are unauthorized collection, private-data processing, credential use, contact with real targets, live system interaction, exploit execution, deception, unsafe cyber-physical action, or external deployment while handling Recon-ng Module Development: Custom Data Source Integration; SpiderFoot Custom Module: Target Intelligence Aggregation.

71.1.4 Python OSINT Library expected artifact package

Section anchor. Section 71.

Expected appendix artifacts are a purpose statement, allowed-inputs card, excluded-actions card, source-lane map, provenance record, claim ledger, safe-substitution note, output schema, review rubric, and capstone handoff memo for Recon-ng Module Development: Custom Data Source Integration; SpiderFoot Custom Module: Target Intelligence Aggregation.

71.1.5 Python OSINT Library safe artifact schema

Section anchor. Section 71.

Field	Required evidence	Reject condition
Purpose	lawful educational, governance, research, or defensive purpose	vague operational objective or missing authority
Inputs	public, official, scholarly, synthetic, owned-lab, or instructor-provided material	private data, live target data, credentialed access, or unclear provenance
Transform	summary, comparison, rubric scoring, tabletop simulation, or audit review	collection expansion, external action, or unsafe system interaction
Output	memo, matrix, checklist, ledger, rubric, or debrief packet	deployable procedure, target package, or automated action plan
Reviewer	human reviewer, approval gate, revision note, and refresh owner	anonymous ownership or no escalation path

71.1.6 Python OSINT Library input/output contract

Section anchor. Section 71.

Contract term	Input rule	Output rule
Source identity	retain `ageintNNN`, title, URL, and checked status	cite with Pandoc keys and avoid pasted raw URLs in prose
Accessibility	include plain-language labels, table headers, and figure alternatives	reject inaccessible figures, unlabeled tables, or single-modality evidence
Rights	identify affected groups, safeguards, and residual risk	preserve privacy, equality, access, contestability, and redress notes
Tooling	use allowlisted tools, visible prompts, logs, and stop conditions	keep outputs evidence-bounded, reversible, and human-reviewed
Refresh	record source, policy, standard, incident, or assessment trigger	assign an owner and date for revalidation

71.1.7 Python OSINT Library failure cases and required responses

Section anchor. Section 71.

Failure case	Signal	Required response
Source laundering	claim cites an agent summary instead of a verified source	rebuild the claim ledger from direct sources
Boundary drift	exercise starts asking for live targets, private data, or external action	stop, substitute synthetic inputs, and document the block
Accessibility gap	learner cannot inspect, navigate, or complete the artifact	remediate and retest before reuse
Rights gap	affected group, safeguard, or redress path is missing	run HRIA/DPIA worksheet and escalate unresolved risk

Failure case	Signal	Required response
Vendor opacity	tool owner, data use, logs, or exit path is unknown	replace tool or pause until procurement evidence exists

71.1.8 Python OSINT Library evidence package schemas

Section anchor. Section 71.

Model and dataset card:

Field	Model card evidence	Dataset card evidence	Review gate
Intended use	accountable task, excluded uses, affected users, human reviewer, and accountable owner	Data Cards purpose statement, recommended use, prohibited reuse, stewardship owner, and affected stakeholder groups	claim is rejected if intended use, excluded use, affected users, or owner is missing
Provenance and collection	model family, version, supplier or lab, training cutoff, deployment context, and configuration hash	upstream source, collection process, annotation method, consent or authority basis, sensitivity class, and license	artifact is held if provenance, license, authority, or collection process is opaque
Composition and limits	capability boundary, known failure modes, tool permissions, context window limits, and unsupported conditions	population, sampling frame, coverage gaps, subgroup visibility, missingness, transformations, and known caveats	artifact is revised if population, coverage, or source limits are invisible
Evaluation and caveats	benchmark suite, task-specific tests, subgroup or context results, red-team findings, uncertainty notes, and failure examples	quality tests, label agreement, bias review, measurement limits, transformation log, and Data Cards answer-evaluation notes	empirical or performance claims are rejected unless test context, subgroup caveats, and uncertainty are visible
Lifecycle controls	release gate, rollback path, monitoring signal, incident threshold, refresh trigger, and model-card update owner	retention rule, access boundary, update cadence, deletion path, stewardship handoff, and dataset-card revision trigger	reuse is blocked without owner, retention, monitoring, rollback, and refresh evidence

Transparency notice:

Step	Artifact	Review gate
Public purpose	plain-language purpose, authority, affected service, and decision role	reader can tell why the system exists and where human judgment remains
Tool and data summary	model, data, supplier, provenance, validation, and accessibility summary	sensitive details are de-sensitized without hiding accountability fields
Impact and review	benefits, risks, safeguards, human review, appeal, and contact point	affected groups can identify recourse and oversight owners
Publication decision	publish, partially publish, delay, or hold decision with exemption rationale	non-public fields have a documented legal, security, privacy, or IP basis

Records retention and audit trail:

Record	Retained fields	Audit question
Source and prompt register	source identity, prompt version, tool allowlist, reviewer, timestamp, and caveat	Can a later reviewer reconstruct the evidentiary path without private or live data?
Decision and exception log	risk owner, accepted exception, compensating control, expiry date, and approval	Is every deviation time-bound, justified, and reviewable?
Artifact retention note	output type, sensitivity, access boundary, deletion rule, and refresh trigger	Does the retention choice match the educational purpose and rights impact?
Incident and remediation record	incident signal, containment action, root cause, owner, retest result, and closure date	Can the same failure be detected and prevented in the next reuse cycle?

Release and change-control gate:

Gate	Release evidence	Block condition
Scope freeze	accountable use case, excluded actions, tool profile, and data boundary	scope expands to external action, live data, or an unreviewed capability
Security and rights review	privacy, accessibility, security, bias, and human-review checks	rights impact, vulnerability, or accessibility issue has no owner
Version and rollback	model or prompt version, changelog, test fixture, and rollback path	change cannot be reproduced, compared, or reverted
Post-release monitoring	monitoring signal, incident threshold, refresh trigger, and owner	deployment or reuse occurs without logging and retest commitments

Risk exception memo:

Field	Minimum content	Approval rule
Exception requested	what requirement cannot be met, why, affected groups, and duration	exception must be specific, time-bound, and tied to a compensating control
Risk basis	likelihood, impact, evidence, uncertainty, alternatives, and rejected options	unsupported confidence or missing alternatives returns the memo for revision
Compensating control	human review, monitoring, access limit, disclosure, remediation, and owner	control must reduce risk without creating an operational workaround
Expiry and retest	expiry date, retest condition, review cadence, and closure criteria	open-ended exceptions are rejected

Learner support and accommodation plan:

Need	Support	Evidence
Access and modality	captions, alt text, keyboard path, plain-language summary, and structured tables	accessibility checklist, defect log, and retest result
Cognitive load	worked examples, staged release, glossary, checklist, and optional practice fixture	UDL design note and learner feedback record
Assessment fairness	allowed-tool statement, AI-use declaration, alternative submission mode, and transparent rubric	assessment-integrity note and accommodation record
Feedback and remediation	revision path, office-hour prompt, example correction, and due-date flexibility policy	feedback log and instructor disposition

Instructor question bank:

Question type	Prompt	Evidence
Source challenge	Which claim would fail if the strongest source were removed or downgraded?	claim ledger revision and source-lane note
Boundary challenge	Where could this exercise drift from analysis into action, and what safe substitute prevents it?	safe-substitution decision and excluded-action card
Rights challenge	Which affected group, accessibility need, privacy interest, or redress path is under-specified?	HRIA/DPIA update and accommodation note
Assurance challenge	What failure would the current evaluation miss, and what retest would reveal it?	adversarial assurance retest and remediation owner

Remediation backlog:

Backlog item	Trigger	Closure evidence
Unverified claim	claim lacks a guide citation or directly verified anchor	verified source, removed claim, or explicit source-guide context note
Unsafe phrasing	wording implies live targeting, external action, exploitation, manipulation, or unsafe control	safe substitute, blocked context, and reviewer sign-off
Accessibility defect	artifact cannot be inspected through an expected assistive or alternative workflow	defect fix, alternative means, and retest result
Assurance gap	evaluation, release, exception, incident, or vendor evidence is incomplete	owner, due date, retest, and accepted disposition

71.1.9 Python OSINT Library rubric scoring bands

Section anchor. Section 71.

Band	Evidence standard	Disposition
4 - ready	source identity, accessibility, rights, safety, and reviewer evidence are complete	may be reused after normal refresh review
3 - revise	one evidence field is incomplete but risk is bounded and remediable	revise before reuse
2 - hold	multiple evidence fields are incomplete or ownership is unclear	hold for instructor and assurance review
1 - reject	unsafe action, private data, inaccessible artifact, or unverified claim appears	reject and rebuild from safe inputs

71.1.10 Python OSINT Library refresh evidence

Section anchor. Section 71.

Evidence item	Refresh trigger	Retained support
Source lane	official source, standard, or legal text changes	checked-as-of date and source note
Safety treatment	operational wording or unsafe motif appears	safe-substitution decision and blocked context
Accessibility	WCAG, UDL, or institutional accessibility duty changes	defect log, retest result, and owner
Rights	privacy, human-rights, public transparency, or education guidance changes	HRIA/DPIA revision note
Vendor/tool	contract, data-use, incident, or model capability changes	procurement packet and incident review

71.1.11 Python OSINT Library validation rubric

Section anchor. Section 71.

Criterion	Passing evidence
Source identity	existing `ageintNNN` keys remain stable or new references are append-only
Verification	official, standards, public-domain, or scholarly URL is checked directly
Safety	method is converted into tabletop, audit, governance, or synthetic-data treatment
Reproducibility	another reviewer can rebuild the artifact from retained inputs
Rights review	privacy, IP, human-rights, workforce, and education impacts are considered where relevant

71.1.12 Python OSINT Library debrief protocol and reuse decision

Section anchor. Section 71.

Debrief by naming what the artifact can support, what it does not establish, what source changed, what risk was avoided by safe substitution, what human approval is still required, and when the appendix should be refreshed for Recon-ng Module Development: Custom Data Source Integration; SpiderFoot Custom Module: Target Intelligence Aggregation.

71.1.13 Python OSINT Library visual navigation and evidence figures: purpose, source flow, and limits

The appendix uses Figure 147 and Figure 10 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 70, Section 72.

71.1.14 Python OSINT Library runtime item map and source roster: generated rows and citation support

Section anchor. Section 71.

Safe curriculum treatment	Blocked source motif, audit-only	Allowed fixture	Rejected action	Required artifact	Citation spine
Custom-source integration governance review using toy records	A.1 retained for audit; operational wording transformed	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	-
Automated-source aggregation governance review using toy records	A.2 retained for audit; operational wording transformed	instructor-provided source cards, toy records, and provenance notes	live collection expansion, tracking, private-data discovery, or targeting	source-quality card and minimization note	-
Search-exposure provenance review using instructor-provided records	A.3 retained for audit; operational wording transformed	instructor-provided source cards, toy records, and provenance notes	live collection expansion, tracking, private-data discovery, or targeting	source-quality card and minimization note	-
Identity-data minimization review using instructor-provided records	A.4 retained for audit; operational wording transformed	sample role records, ethics cards, and reviewer notes	impersonation, contact activity, elicitation, handling, or source exposure	source-protection ethics memo and escalation path	-
Social-source provenance and minimization review using toy records	A.5 retained for audit; operational wording transformed	instructor-provided source cards, toy records, and provenance notes	live collection expansion, tracking, private-data discovery, or targeting	source-quality card and minimization note	-
IP-geolocation uncertainty review using synthetic records	A.6 retained for audit; operational wording transformed	provided imagery metadata, synthetic change examples, and uncertainty notes	live collection expansion, tracking, private-data discovery, or targeting	source-quality card and minimization note	-
Sandbox policy and tool-isolation review using toy OSINT fixtures	A.7 retained for audit; operational wording transformed	toy OSINT fixtures, sandbox policy cards, and blocked-action logs	external execution, credentialed access, network calls, or unmanaged tool use	tool-isolation run card and denied-action evidence	-

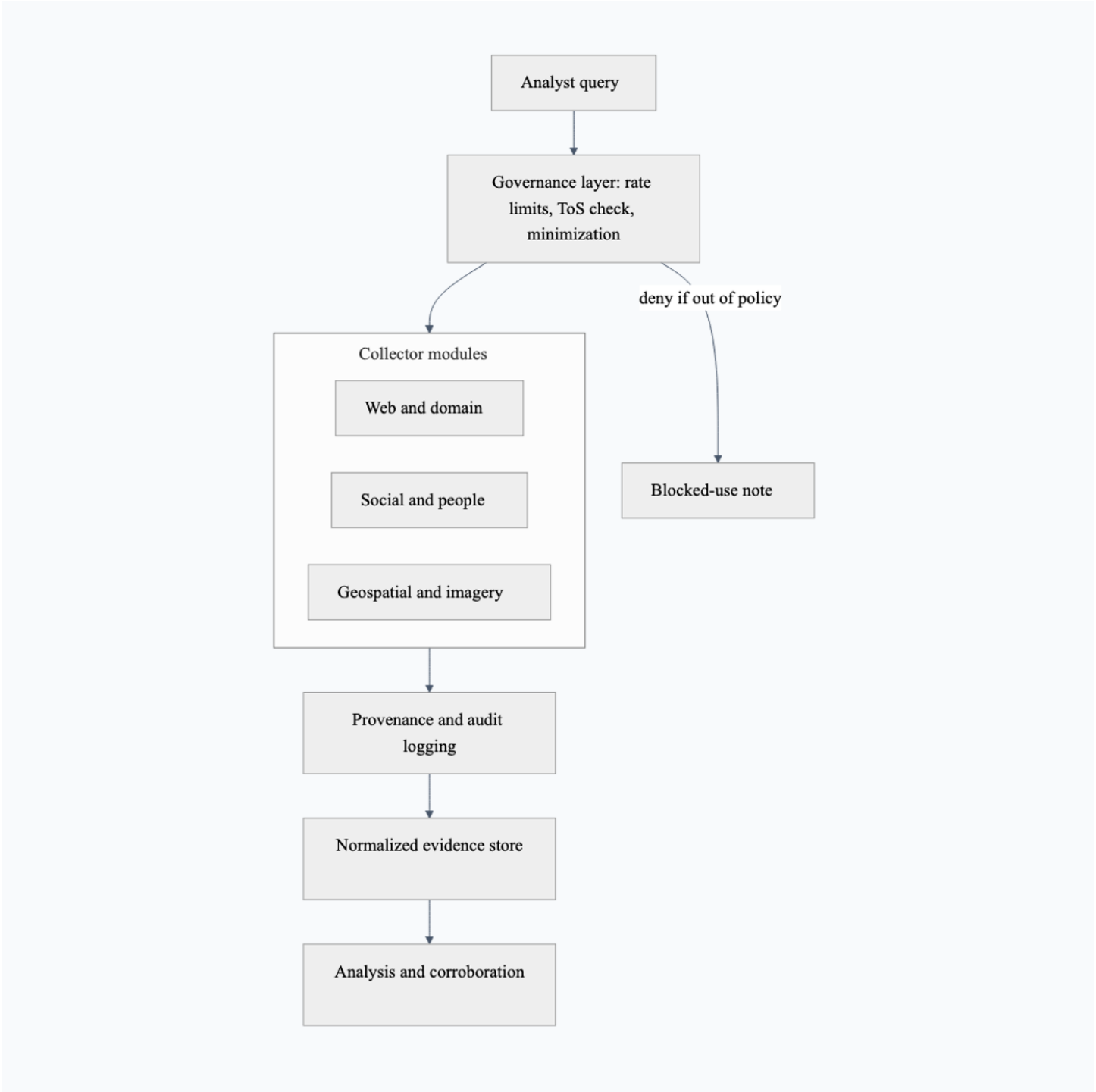


Figure 147: The reference OSINT library is organized as governed modules where every collector passes through rate-limiting, minimization, and provenance logging before results reach analysis. It is anchored to the python osint library appendix; use it to inspect Analyst query, Governance layer: rate limits, ToS check, minimization, Collector modules, and Web and domain while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

72 LangChain/LangGraph AGEINT Patterns

The current appendix is an evidence workbook for reusable classroom methods. It is educational and evidence-bounded: examples remain synthetic, defensive, lawful, and bounded to owned labs, public sources, or tabletop exercises. Source-item focus: ReAct Agent for Threat Intelligence Enrichment (MITRE ATT&CK + VirusTotal); LangGraph State Machine: Multi-Phase Intelligence Collection DAG.

72.1 LangChain/LangGraph AGEINT Patterns workbook scope: purpose, safety envelope, and reuse decision

Section anchor. Section 72.

72.1.1 LangChain/LangGraph AGEINT Patterns operating purpose

Section anchor. Section 72.

The current appendix supports a reusable methods workbook. Each source item is treated as a reviewable classroom artifact rather than an operational instruction; examples begin with ReAct Agent for Threat Intelligence Enrichment (MITRE ATT&CK + VirusTotal); LangGraph State Machine: Multi-Phase Intelligence Collection DAG.

72.1.2 LangChain/LangGraph AGEINT Patterns allowed-input boundary

Section anchor. Section 72.

Allowed inputs for the current appendix are public official or scholarly sources, standards text, instructor-provided excerpts, synthetic datasets, owned-lab logs, toy examples, and generated rubrics that expose their provenance for ReAct Agent for Threat Intelligence Enrichment (MITRE ATT&CK + VirusTotal); LangGraph State Machine: Multi-Phase Intelligence Collection DAG.

72.1.3 LangChain/LangGraph AGEINT Patterns excluded-action boundary

Section anchor. Section 72.

Excluded actions for the current appendix are unauthorized collection, private-data processing, credential use, contact with real targets, live system interaction, exploit execution, deception, unsafe cyber-physical action, or external deployment while handling ReAct Agent for Threat Intelligence Enrichment (MITRE ATT&CK + VirusTotal); LangGraph State Machine: Multi-Phase Intelligence Collection DAG.

72.1.4 LangChain/LangGraph AGEINT Patterns expected artifact package

Section anchor. Section 72.

Expected appendix artifacts are a purpose statement, allowed-inputs card, excluded-actions card, source-lane map, provenance record, claim ledger, safe-substitution note, output schema, review rubric, and capstone handoff memo for ReAct Agent for Threat Intelligence Enrichment (MITRE ATT&CK + VirusTotal); LangGraph State Machine: Multi-Phase Intelligence Collection DAG.

72.1.5 LangChain/LangGraph AGEINT Patterns safe artifact schema

Section anchor. Section 72.

Field	Required evidence	Reject condition
Purpose	lawful educational, governance, research, or defensive purpose	vague operational objective or missing authority
Inputs	public, official, scholarly, synthetic, owned-lab, or instructor-provided material	private data, live target data, credentialed access, or unclear provenance
Transform	summary, comparison, rubric scoring, tabletop simulation, or audit review	collection expansion, external action, or unsafe system interaction
Output	memo, matrix, checklist, ledger, rubric, or debrief packet	deployable procedure, target package, or automated action plan
Reviewer	human reviewer, approval gate, revision note, and refresh owner	anonymous ownership or no escalation path

72.1.6 LangChain/LangGraph AGEINT Patterns input/output contract

Section anchor. Section 72.

Contract term	Input rule	Output rule
Source identity	retain `ageintNNN`, title, URL, and checked status	cite with Pandoc keys and avoid pasted raw URLs in prose
Accessibility	include plain-language labels, table headers, and figure alternatives	reject inaccessible figures, unlabeled tables, or single-modality evidence
Rights	identify affected groups, safeguards, and residual risk	preserve privacy, equality, access, contestability, and redress notes
Tooling	use allowlisted tools, visible prompts, logs, and stop conditions	keep outputs evidence-bounded, reversible, and human-reviewed
Refresh	record source, policy, standard, incident, or assessment trigger	assign an owner and date for revalidation

72.1.7 LangChain/LangGraph AGEINT Patterns failure cases and required responses

Section anchor. Section 72.

Failure case	Signal	Required response
Source laundering	claim cites an agent summary instead of a verified source	rebuild the claim ledger from direct sources
Boundary drift	exercise starts asking for live targets, private data, or external action	stop, substitute synthetic inputs, and document the block
Accessibility gap	learner cannot inspect, navigate, or complete the artifact	remediate and retest before reuse
Rights gap	affected group, safeguard, or redress path is missing	run HRIA/DPIA worksheet and escalate unresolved risk

Failure case	Signal	Required response
Vendor opacity	tool owner, data use, logs, or exit path is unknown	replace tool or pause until procurement evidence exists

72.1.8 LangChain/LangGraph AGEINT Patterns evidence package schemas

Section anchor. Section 72.

Model and dataset card:

Field	Model card evidence	Dataset card evidence	Review gate
Intended use	accountable task, excluded uses, affected users, human reviewer, and accountable owner	Data Cards purpose statement, recommended use, prohibited reuse, stewardship owner, and affected stakeholder groups	claim is rejected if intended use, excluded use, affected users, or owner is missing
Provenance and collection	model family, version, supplier or lab, training cutoff, deployment context, and configuration hash	upstream source, collection process, annotation method, consent or authority basis, sensitivity class, and license	artifact is held if provenance, license, authority, or collection process is opaque
Composition and limits	capability boundary, known failure modes, tool permissions, context window limits, and unsupported conditions	population, sampling frame, coverage gaps, subgroup visibility, missingness, transformations, and known caveats	artifact is revised if population, coverage, or source limits are invisible
Evaluation and caveats	benchmark suite, task-specific tests, subgroup or context results, red-team findings, uncertainty notes, and failure examples	quality tests, label agreement, bias review, measurement limits, transformation log, and Data Cards answer-evaluation notes	empirical or performance claims are rejected unless test context, subgroup caveats, and uncertainty are visible
Lifecycle controls	release gate, rollback path, monitoring signal, incident threshold, refresh trigger, and model-card update owner	retention rule, access boundary, update cadence, deletion path, stewardship handoff, and dataset-card revision trigger	reuse is blocked without owner, retention, monitoring, rollback, and refresh evidence

Transparency notice:

Step	Artifact	Review gate
Public purpose	plain-language purpose, authority, affected service, and decision role	reader can tell why the system exists and where human judgment remains
Tool and data summary	model, data, supplier, provenance, validation, and accessibility summary	sensitive details are de-sensitized without hiding accountability fields
Impact and review	benefits, risks, safeguards, human review, appeal, and contact point	affected groups can identify recourse and oversight owners
Publication decision	publish, partially publish, delay, or hold decision with exemption rationale	non-public fields have a documented legal, security, privacy, or IP basis

Records retention and audit trail:

Record	Retained fields	Audit question
Source and prompt register	source identity, prompt version, tool allowlist, reviewer, timestamp, and caveat	Can a later reviewer reconstruct the evidentiary path without private or live data?
Decision and exception log	risk owner, accepted exception, compensating control, expiry date, and approval	Is every deviation time-bound, justified, and reviewable?
Artifact retention note	output type, sensitivity, access boundary, deletion rule, and refresh trigger	Does the retention choice match the educational purpose and rights impact?
Incident and remediation record	incident signal, containment action, root cause, owner, retest result, and closure date	Can the same failure be detected and prevented in the next reuse cycle?

Release and change-control gate:

Gate	Release evidence	Block condition
Scope freeze	accountable use case, excluded actions, tool profile, and data boundary	scope expands to external action, live data, or an unreviewed capability
Security and rights review	privacy, accessibility, security, bias, and human-review checks	rights impact, vulnerability, or accessibility issue has no owner
Version and rollback	model or prompt version, changelog, test fixture, and rollback path	change cannot be reproduced, compared, or reverted
Post-release monitoring	monitoring signal, incident threshold, refresh trigger, and owner	deployment or reuse occurs without logging and retest commitments

Risk exception memo:

Field	Minimum content	Approval rule
Exception requested	what requirement cannot be met, why, affected groups, and duration	exception must be specific, time-bound, and tied to a compensating control
Risk basis	likelihood, impact, evidence, uncertainty, alternatives, and rejected options	unsupported confidence or missing alternatives returns the memo for revision
Compensating control	human review, monitoring, access limit, disclosure, remediation, and owner	control must reduce risk without creating an operational workaround
Expiry and retest	expiry date, retest condition, review cadence, and closure criteria	open-ended exceptions are rejected

Learner support and accommodation plan:

Need	Support	Evidence
Access and modality	captions, alt text, keyboard path, plain-language summary, and structured tables	accessibility checklist, defect log, and retest result
Cognitive load	worked examples, staged release, glossary, checklist, and optional practice fixture	UDL design note and learner feedback record
Assessment fairness	allowed-tool statement, AI-use declaration, alternative submission mode, and transparent rubric	assessment-integrity note and accommodation record
Feedback and remediation	revision path, office-hour prompt, example correction, and due-date flexibility policy	feedback log and instructor disposition

Instructor question bank:

Question type	Prompt	Evidence
Source challenge	Which claim would fail if the strongest source were removed or downgraded?	claim ledger revision and source-lane note
Boundary challenge	Where could this exercise drift from analysis into action, and what safe substitute prevents it?	safe-substitution decision and excluded-action card
Rights challenge	Which affected group, accessibility need, privacy interest, or redress path is under-specified?	HRIA/DPIA update and accommodation note
Assurance challenge	What failure would the current evaluation miss, and what retest would reveal it?	adversarial assurance retest and remediation owner

Remediation backlog:

Backlog item	Trigger	Closure evidence
Unverified claim	claim lacks a guide citation or directly verified anchor	verified source, removed claim, or explicit source-guide context note
Unsafe phrasing	wording implies live targeting, external action, exploitation, manipulation, or unsafe control	safe substitute, blocked context, and reviewer sign-off
Accessibility defect	artifact cannot be inspected through an expected assistive or alternative workflow	defect fix, alternative means, and retest result
Assurance gap	evaluation, release, exception, incident, or vendor evidence is incomplete	owner, due date, retest, and accepted disposition

72.1.9 LangChain/LangGraph AGEINT Patterns rubric scoring bands

Section anchor. Section 72.

Band	Evidence standard	Disposition
4 - ready	source identity, accessibility, rights, safety, and reviewer evidence are complete	may be reused after normal refresh review
3 - revise	one evidence field is incomplete but risk is bounded and remediable	revise before reuse
2 - hold	multiple evidence fields are incomplete or ownership is unclear	hold for instructor and assurance review
1 - reject	unsafe action, private data, inaccessible artifact, or unverified claim appears	reject and rebuild from safe inputs

72.1.10 LangChain/LangGraph AGEINT Patterns refresh evidence

Section anchor. Section 72.

Evidence item	Refresh trigger	Retained support
Source lane	official source, standard, or legal text changes	checked-as-of date and source note
Safety treatment	operational wording or unsafe motif appears	safe-substitution decision and blocked context
Accessibility	WCAG, UDL, or institutional accessibility duty changes	defect log, retest result, and owner
Rights	privacy, human-rights, public transparency, or education guidance changes	HRIA/DPIA revision note
Vendor/tool	contract, data-use, incident, or model capability changes	procurement packet and incident review

72.1.11 LangChain/LangGraph AGEINT Patterns validation rubric

Section anchor. Section 72.

Criterion	Passing evidence
Source identity	existing `ageintNNN` keys remain stable or new references are append-only
Verification	official, standards, public-domain, or scholarly URL is checked directly
Safety	method is converted into tabletop, audit, governance, or synthetic-data treatment
Reproducibility	another reviewer can rebuild the artifact from retained inputs
Rights review	privacy, IP, human-rights, workforce, and education impacts are considered where relevant

72.1.12 LangChain/LangGraph AGEINT Patterns debrief protocol and reuse decision

Section anchor. Section 72.

Debrief by naming what the artifact can support, what it does not establish, what source changed, what risk was avoided by safe substitution, what human approval is still required, and when the appendix should be refreshed for ReAct Agent for Threat Intelligence Enrichment (MITRE ATT&CK + VirusTotal); LangGraph State Machine: Multi-Phase Intelligence Collection DAG.

72.1.13 LangChain/LangGraph AGEINT Patterns visual navigation and evidence figures: purpose, source flow, and limits

The appendix uses Figure 148 and Figure 10 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 71, Section 73.

72.1.14 LangChain/LangGraph AGEINT Patterns runtime item map and source roster: generated rows and citation support

Section anchor. Section 72.

Safe curriculum treatment	Blocked source motif, audit-only	Allowed fixture	Rejected action	Required artifact	Citation spine
B.1 ReAct Agent for Threat Intelligence Enrichment (MITRE ATT&CK + VirusTotal)	no blocked motif; source title used verbatim	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	-
B.2 LangGraph State Machine: Multi-Phase Intelligence Collection DAG	no blocked motif; source title used verbatim	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	-
B.3 RAG Pipeline: All-Source Fusion over STIX + PDF Intelligence Products	no blocked motif; source title used verbatim	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	-
B.4 Human-in-the-Loop Agent with Confidence-Gated Escalation	no blocked motif; source title used verbatim	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	-
Claim-ledger memory exercise that tracks evidence changes rather than people	B.5 retained for audit; operational wording transformed	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	-
B.6 LangSmith Tracing: Observability for Production Intelligence Agents	no blocked motif; source title used verbatim	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	-

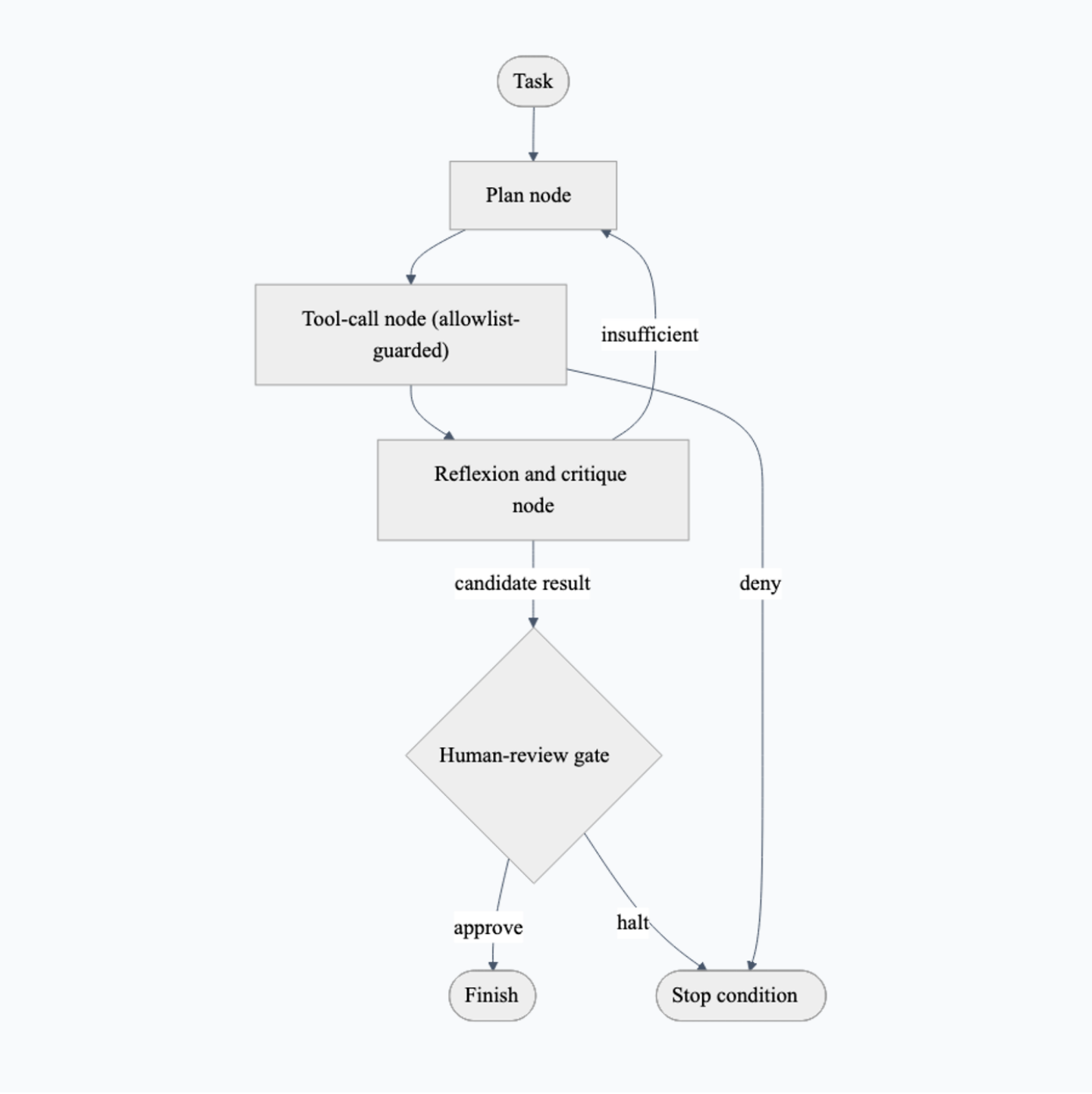


Figure 148: The LangGraph pattern models an agent as a state machine where a reflexion node and a human-review gate bound every tool action before the graph can advance or finish. Its reader value is to make Task, Plan node, Tool-call node (allowlist-guarded), and Reflexion and critique node visible at a glance, with the langchain langgraph ageint patterns appendix as the source section and defensive review as the boundary.

73 CrewAI Multi-Agent Operations

The current appendix is an evidence workbook for reusable classroom methods. It is educational and evidence-bounded: examples remain synthetic, defensive, lawful, and bounded to owned labs, public sources, or tabletop exercises. Source-item focus: OSINT Crew: 5-Agent System (Planner, OSINT Collector, SIGINT, Analyst, Reporter); Red/Blue Cell Debate Crew: Automated ACH with Adversarial Agents.

73.1 CrewAI Multi-Agent Operations workbook scope: purpose, safety envelope, and reuse decision

Section anchor. Section 73.

73.1.1 CrewAI Multi-Agent Operations operating purpose

Section anchor. Section 73.

The current appendix supports a reusable methods workbook. Each source item is treated as a reviewable classroom artifact rather than an operational instruction; examples begin with OSINT Crew: 5-Agent System (Planner, OSINT Collector, SIGINT, Analyst, Reporter); Red/Blue Cell Debate Crew: Automated ACH with Adversarial Agents.

73.1.2 CrewAI Multi-Agent Operations allowed-input boundary

Section anchor. Section 73.

Allowed inputs for the current appendix are public official or scholarly sources, standards text, instructor-provided excerpts, synthetic datasets, owned-lab logs, toy examples, and generated rubrics that expose their provenance for OSINT Crew: 5-Agent System (Planner, OSINT Collector, SIGINT, Analyst, Reporter); Red/Blue Cell Debate Crew: Automated ACH with Adversarial Agents.

73.1.3 CrewAI Multi-Agent Operations excluded-action boundary

Section anchor. Section 73.

Excluded actions for the current appendix are unauthorized collection, private-data processing, credential use, contact with real targets, live system interaction, exploit execution, deception, unsafe cyber-physical action, or external deployment while handling OSINT Crew: 5-Agent System (Planner, OSINT Collector, SIGINT, Analyst, Reporter); Red/Blue Cell Debate Crew: Automated ACH with Adversarial Agents.

73.1.4 CrewAI Multi-Agent Operations expected artifact package

Section anchor. Section 73.

Expected appendix artifacts are a purpose statement, allowed-inputs card, excluded-actions card, source-lane map, provenance record, claim ledger, safe-substitution note, output schema, review rubric, and capstone handoff memo for OSINT Crew: 5-Agent System (Planner, OSINT Collector, SIGINT, Analyst, Reporter); Red/Blue Cell Debate Crew: Automated ACH with Adversarial Agents.

73.1.5 CrewAI Multi-Agent Operations safe artifact schema

Section anchor. Section 73.

Field	Required evidence	Reject condition
Purpose	lawful educational, governance, research, or defensive purpose	vague operational objective or missing authority
Inputs	public, official, scholarly, synthetic, owned-lab, or instructor-provided material	private data, live target data, credentialed access, or unclear provenance
Transform	summary, comparison, rubric scoring, tabletop simulation, or audit review	collection expansion, external action, or unsafe system interaction
Output	memo, matrix, checklist, ledger, rubric, or debrief packet	deployable procedure, target package, or automated action plan
Reviewer	human reviewer, approval gate, revision note, and refresh owner	anonymous ownership or no escalation path

73.1.6 CrewAI Multi-Agent Operations input/output contract

Section anchor. Section 73.

Contract term	Input rule	Output rule
Source identity	retain `ageintNNN`, title, URL, and checked status	cite with Pandoc keys and avoid pasted raw URLs in prose
Accessibility	include plain-language labels, table headers, and figure alternatives	reject inaccessible figures, unlabeled tables, or single-modality evidence
Rights	identify affected groups, safeguards, and residual risk	preserve privacy, equality, access, contestability, and redress notes
Tooling	use allowlisted tools, visible prompts, logs, and stop conditions	keep outputs evidence-bounded, reversible, and human-reviewed
Refresh	record source, policy, standard, incident, or assessment trigger	assign an owner and date for revalidation

73.1.7 CrewAI Multi-Agent Operations failure cases and required responses

Section anchor. Section 73.

Failure case	Signal	Required response
Source laundering	claim cites an agent summary instead of a verified source	rebuild the claim ledger from direct sources
Boundary drift	exercise starts asking for live targets, private data, or external action	stop, substitute synthetic inputs, and document the block
Accessibility gap	learner cannot inspect, navigate, or complete the artifact	remediate and retest before reuse
Rights gap	affected group, safeguard, or redress path is missing	run HRIA/DPIA worksheet and escalate unresolved risk

Failure case	Signal	Required response
Vendor opacity	tool owner, data use, logs, or exit path is unknown	replace tool or pause until procurement evidence exists

73.1.8 CrewAI Multi-Agent Operations evidence package schemas

Section anchor. Section 73.

Model and dataset card:

Field	Model card evidence	Dataset card evidence	Review gate
Intended use	accountable task, excluded uses, affected users, human reviewer, and accountable owner	Data Cards purpose statement, recommended use, prohibited reuse, stewardship owner, and affected stakeholder groups	claim is rejected if intended use, excluded use, affected users, or owner is missing
Provenance and collection	model family, version, supplier or lab, training cutoff, deployment context, and configuration hash	upstream source, collection process, annotation method, consent or authority basis, sensitivity class, and license	artifact is held if provenance, license, authority, or collection process is opaque
Composition and limits	capability boundary, known failure modes, tool permissions, context window limits, and unsupported conditions	population, sampling frame, coverage gaps, subgroup visibility, missingness, transformations, and known caveats	artifact is revised if population, coverage, or source limits are invisible
Evaluation and caveats	benchmark suite, task-specific tests, subgroup or context results, red-team findings, uncertainty notes, and failure examples	quality tests, label agreement, bias review, measurement limits, transformation log, and Data Cards answer-evaluation notes	empirical or performance claims are rejected unless test context, subgroup caveats, and uncertainty are visible
Lifecycle controls	release gate, rollback path, monitoring signal, incident threshold, refresh trigger, and model-card update owner	retention rule, access boundary, update cadence, deletion path, stewardship handoff, and dataset-card revision trigger	reuse is blocked without owner, retention, monitoring, rollback, and refresh evidence

Transparency notice:

Step	Artifact	Review gate
Public purpose	plain-language purpose, authority, affected service, and decision role	reader can tell why the system exists and where human judgment remains
Tool and data summary	model, data, supplier, provenance, validation, and accessibility summary	sensitive details are de-sensitized without hiding accountability fields
Impact and review	benefits, risks, safeguards, human review, appeal, and contact point	affected groups can identify recourse and oversight owners
Publication decision	publish, partially publish, delay, or hold decision with exemption rationale	non-public fields have a documented legal, security, privacy, or IP basis

Records retention and audit trail:

Record	Retained fields	Audit question
Source and prompt register	source identity, prompt version, tool allowlist, reviewer, timestamp, and caveat	Can a later reviewer reconstruct the evidentiary path without private or live data?
Decision and exception log	risk owner, accepted exception, compensating control, expiry date, and approval	Is every deviation time-bound, justified, and reviewable?
Artifact retention note	output type, sensitivity, access boundary, deletion rule, and refresh trigger	Does the retention choice match the educational purpose and rights impact?
Incident and remediation record	incident signal, containment action, root cause, owner, retest result, and closure date	Can the same failure be detected and prevented in the next reuse cycle?

Release and change-control gate:

Gate	Release evidence	Block condition
Scope freeze	accountable use case, excluded actions, tool profile, and data boundary	scope expands to external action, live data, or an unreviewed capability
Security and rights review	privacy, accessibility, security, bias, and human-review checks	rights impact, vulnerability, or accessibility issue has no owner
Version and rollback	model or prompt version, changelog, test fixture, and rollback path	change cannot be reproduced, compared, or reverted
Post-release monitoring	monitoring signal, incident threshold, refresh trigger, and owner	deployment or reuse occurs without logging and retest commitments

Risk exception memo:

Field	Minimum content	Approval rule
Exception requested	what requirement cannot be met, why, affected groups, and duration	exception must be specific, time-bound, and tied to a compensating control
Risk basis	likelihood, impact, evidence, uncertainty, alternatives, and rejected options	unsupported confidence or missing alternatives returns the memo for revision
Compensating control	human review, monitoring, access limit, disclosure, remediation, and owner	control must reduce risk without creating an operational workaround
Expiry and retest	expiry date, retest condition, review cadence, and closure criteria	open-ended exceptions are rejected

Learner support and accommodation plan:

Need	Support	Evidence
Access and modality	captions, alt text, keyboard path, plain-language summary, and structured tables	accessibility checklist, defect log, and retest result
Cognitive load	worked examples, staged release, glossary, checklist, and optional practice fixture	UDL design note and learner feedback record
Assessment fairness	allowed-tool statement, AI-use declaration, alternative submission mode, and transparent rubric	assessment-integrity note and accommodation record
Feedback and remediation	revision path, office-hour prompt, example correction, and due-date flexibility policy	feedback log and instructor disposition

Instructor question bank:

Question type	Prompt	Evidence
Source challenge	Which claim would fail if the strongest source were removed or downgraded?	claim ledger revision and source-lane note
Boundary challenge	Where could this exercise drift from analysis into action, and what safe substitute prevents it?	safe-substitution decision and excluded-action card
Rights challenge	Which affected group, accessibility need, privacy interest, or redress path is under-specified?	HRIA/DPIA update and accommodation note
Assurance challenge	What failure would the current evaluation miss, and what retest would reveal it?	adversarial assurance retest and remediation owner

Remediation backlog:

Backlog item	Trigger	Closure evidence
Unverified claim	claim lacks a guide citation or directly verified anchor	verified source, removed claim, or explicit source-guide context note
Unsafe phrasing	wording implies live targeting, external action, exploitation, manipulation, or unsafe control	safe substitute, blocked context, and reviewer sign-off
Accessibility defect	artifact cannot be inspected through an expected assistive or alternative workflow	defect fix, alternative means, and retest result
Assurance gap	evaluation, release, exception, incident, or vendor evidence is incomplete	owner, due date, retest, and accepted disposition

73.1.9 CrewAI Multi-Agent Operations rubric scoring bands

Section anchor. Section 73.

Band	Evidence standard	Disposition
4 - ready	source identity, accessibility, rights, safety, and reviewer evidence are complete	may be reused after normal refresh review
3 - revise	one evidence field is incomplete but risk is bounded and remediable	revise before reuse
2 - hold	multiple evidence fields are incomplete or ownership is unclear	hold for instructor and assurance review
1 - reject	unsafe action, private data, inaccessible artifact, or unverified claim appears	reject and rebuild from safe inputs

73.1.10 CrewAI Multi-Agent Operations refresh evidence

Section anchor. Section 73.

Evidence item	Refresh trigger	Retained support
Source lane	official source, standard, or legal text changes	checked-as-of date and source note
Safety treatment	operational wording or unsafe motif appears	safe-substitution decision and blocked context
Accessibility	WCAG, UDL, or institutional accessibility duty changes	defect log, retest result, and owner
Rights	privacy, human-rights, public transparency, or education guidance changes	HRIA/DPIA revision note
Vendor/tool	contract, data-use, incident, or model capability changes	procurement packet and incident review

73.1.11 CrewAI Multi-Agent Operations validation rubric

Section anchor. Section 73.

Criterion	Passing evidence
Source identity	existing `ageintNNN` keys remain stable or new references are append-only
Verification	official, standards, public-domain, or scholarly URL is checked directly
Safety	method is converted into tabletop, audit, governance, or synthetic-data treatment
Reproducibility	another reviewer can rebuild the artifact from retained inputs
Rights review	privacy, IP, human-rights, workforce, and education impacts are considered where relevant

73.1.12 CrewAI Multi-Agent Operations debrief protocol and reuse decision

Section anchor. Section 73.

Debrief by naming what the artifact can support, what it does not establish, what source changed, what risk was avoided by safe substitution, what human approval is still required, and when the appendix should be refreshed for OSINT Crew: 5-Agent System (Planner, OSINT Collector, SIGINT, Analyst, Reporter); Red/Blue Cell Debate Crew: Automated ACH with Adversarial Agents.

73.1.13 CrewAI Multi-Agent Operations visual navigation and evidence figures: purpose, source flow, and limits

The appendix uses Figure 149 and Figure 10 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 72, Section 74.

73.1.14 CrewAI Multi-Agent Operations runtime item map and source roster: generated rows and citation support

Section anchor. Section 73.

Safe curriculum treatment	Blocked source motif, audit-only	Allowed fixture	Rejected action	Required artifact	Citation spine
C.1 OSINT Crew: 5-Agent System (Planner, OSINT Collector, SIGINT, Analyst, Reporter)	no blocked motif; source title used verbatim	instructor-provided source cards, toy records, and provenance notes	live collection expansion, tracking, private-data discovery, or targeting	source-quality card and minimization note	-
C.2 Red/Blue Cell Debate Crew: Automated ACH with Adversarial Agents	no blocked motif; source title used verbatim	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	-
C.3 ICS Anomaly Investigation Crew: OT + MITRE ATT&CK for ICS Tools	no blocked motif; source title used verbatim	synthetic process logs, operator-decision cards, and safety stop rules	live device interaction, process manipulation, unsafe actuation, or plant operation	tabletop packet with asset, consequence, operator decision, and recovery evidence	-
Psychological inoculation and prebunking literacy review	C.4 retained for audit; operational wording transformed	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	-

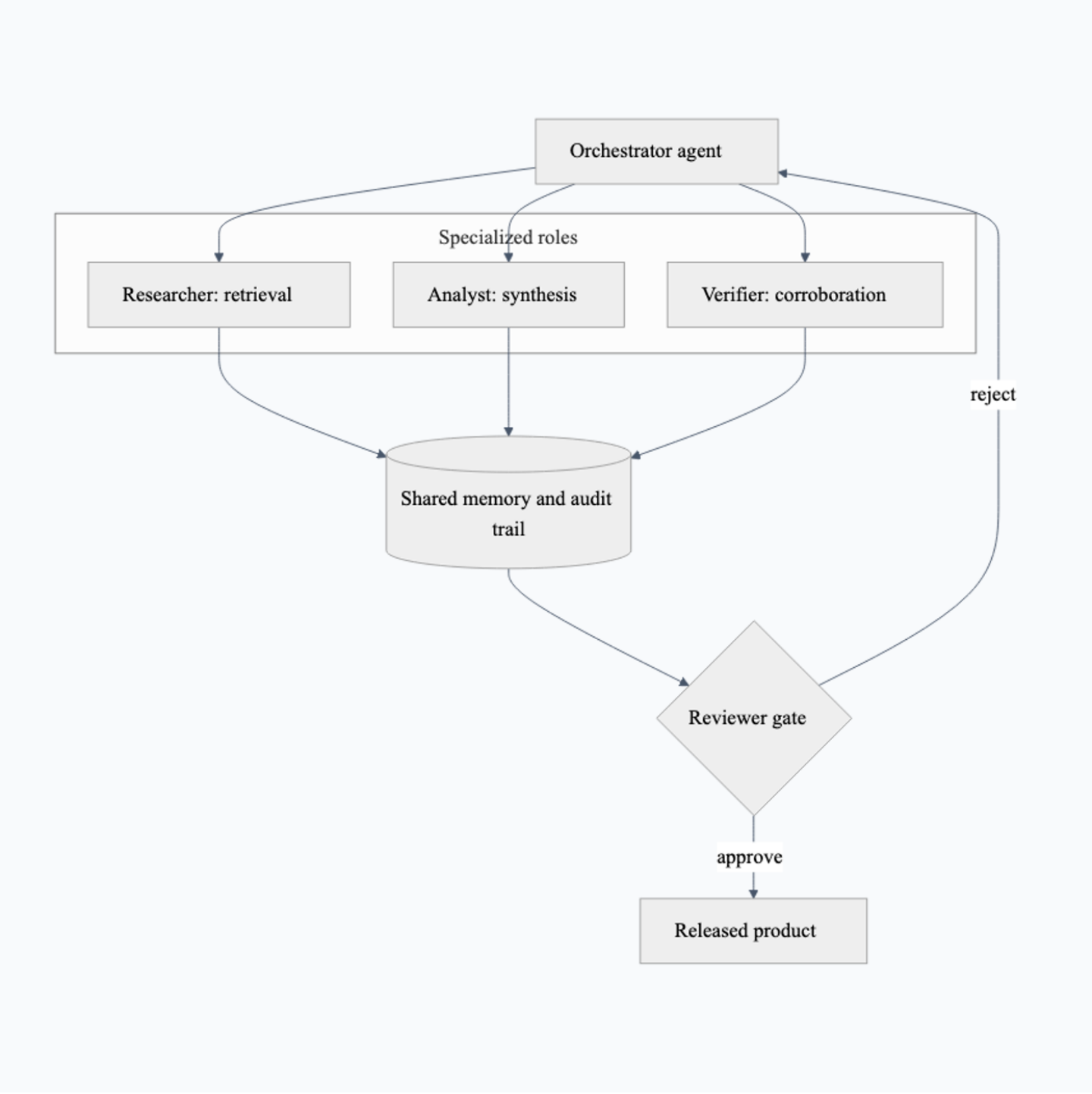


Figure 149: The multi-agent crew separates duties across specialized roles coordinated by an orchestrator, with a reviewer role and shared memory enforcing accountability before any output is released. The captioned view belongs to the crewai multi agent operations appendix and should be read as a map of Orchestrator agent, Specialized roles, Researcher: retrieval, and Analyst: synthesis, not as a capability score or live-task instruction.

74 AutoGen and MCP Patterns

The current appendix is an evidence workbook for reusable classroom methods. It is educational and evidence-bounded: examples remain synthetic, defensive, lawful, and bounded to owned labs, public sources, or tabletop exercises. Source-item focus: AutoGen Code-Execution Exploit Chain (with Sandboxing Countermeasure); MCP Server: Building a STIX/TAXII Intelligence Tool Server.

74.1 AutoGen and MCP Patterns workbook scope: purpose, safety envelope, and reuse decision

Section anchor. Section 74.

74.1.1 AutoGen and MCP Patterns operating purpose

Section anchor. Section 74.

The current appendix supports a reusable methods workbook. Each source item is treated as a reviewable classroom artifact rather than an operational instruction; examples begin with AutoGen Code-Execution Exploit Chain (with Sandboxing Countermeasure); MCP Server: Building a STIX/TAXII Intelligence Tool Server.

74.1.2 AutoGen and MCP Patterns allowed-input boundary

Section anchor. Section 74.

Allowed inputs for the current appendix are public official or scholarly sources, standards text, instructor-provided excerpts, synthetic datasets, owned-lab logs, toy examples, and generated rubrics that expose their provenance for AutoGen Code-Execution Exploit Chain (with Sandboxing Countermeasure); MCP Server: Building a STIX/TAXII Intelligence Tool Server.

74.1.3 AutoGen and MCP Patterns excluded-action boundary

Section anchor. Section 74.

Excluded actions for the current appendix are unauthorized collection, private-data processing, credential use, contact with real targets, live system interaction, exploit execution, deception, unsafe cyber-physical action, or external deployment while handling AutoGen Code-Execution Exploit Chain (with Sandboxing Countermeasure); MCP Server: Building a STIX/TAXII Intelligence Tool Server.

74.1.4 AutoGen and MCP Patterns expected artifact package

Section anchor. Section 74.

Expected appendix artifacts are a purpose statement, allowed-inputs card, excluded-actions card, source-lane map, provenance record, claim ledger, safe-substitution note, output schema, review rubric, and capstone handoff memo for AutoGen Code-Execution Exploit Chain (with Sandboxing Countermeasure); MCP Server: Building a STIX/TAXII Intelligence Tool Server.

74.1.5 AutoGen and MCP Patterns safe artifact schema

Section anchor. Section 74.

Field	Required evidence	Reject condition
Purpose	lawful educational, governance, research, or defensive purpose	vague operational objective or missing authority
Inputs	public, official, scholarly, synthetic, owned-lab, or instructor-provided material	private data, live target data, credentialed access, or unclear provenance
Transform	summary, comparison, rubric scoring, tabletop simulation, or audit review	collection expansion, external action, or unsafe system interaction
Output	memo, matrix, checklist, ledger, rubric, or debrief packet	deployable procedure, target package, or automated action plan
Reviewer	human reviewer, approval gate, revision note, and refresh owner	anonymous ownership or no escalation path

74.1.6 AutoGen and MCP Patterns input/output contract

Section anchor. Section 74.

Contract term	Input rule	Output rule
Source identity	retain `ageintNNN`, title, URL, and checked status	cite with Pandoc keys and avoid pasted raw URLs in prose
Accessibility	include plain-language labels, table headers, and figure alternatives	reject inaccessible figures, unlabeled tables, or single-modality evidence
Rights	identify affected groups, safeguards, and residual risk	preserve privacy, equality, access, contestability, and redress notes
Tooling	use allowlisted tools, visible prompts, logs, and stop conditions	keep outputs evidence-bounded, reversible, and human-reviewed
Refresh	record source, policy, standard, incident, or assessment trigger	assign an owner and date for revalidation

74.1.7 AutoGen and MCP Patterns failure cases and required responses

Section anchor. Section 74.

Failure case	Signal	Required response
Source laundering	claim cites an agent summary instead of a verified source	rebuild the claim ledger from direct sources
Boundary drift	exercise starts asking for live targets, private data, or external action	stop, substitute synthetic inputs, and document the block
Accessibility gap	learner cannot inspect, navigate, or complete the artifact	remediate and retest before reuse
Rights gap	affected group, safeguard, or redress path is missing	run HRIA/DPIA worksheet and escalate unresolved risk

Failure case	Signal	Required response
Vendor opacity	tool owner, data use, logs, or exit path is unknown	replace tool or pause until procurement evidence exists

74.1.8 AutoGen and MCP Patterns evidence package schemas

Section anchor. Section 74.

Model and dataset card:

Field	Model card evidence	Dataset card evidence	Review gate
Intended use	accountable task, excluded uses, affected users, human reviewer, and accountable owner	Data Cards purpose statement, recommended use, prohibited reuse, stewardship owner, and affected stakeholder groups	claim is rejected if intended use, excluded use, affected users, or owner is missing
Provenance and collection	model family, version, supplier or lab, training cutoff, deployment context, and configuration hash	upstream source, collection process, annotation method, consent or authority basis, sensitivity class, and license	artifact is held if provenance, license, authority, or collection process is opaque
Composition and limits	capability boundary, known failure modes, tool permissions, context window limits, and unsupported conditions	population, sampling frame, coverage gaps, subgroup visibility, missingness, transformations, and known caveats	artifact is revised if population, coverage, or source limits are invisible
Evaluation and caveats	benchmark suite, task-specific tests, subgroup or context results, red-team findings, uncertainty notes, and failure examples	quality tests, label agreement, bias review, measurement limits, transformation log, and Data Cards answer-evaluation notes	empirical or performance claims are rejected unless test context, subgroup caveats, and uncertainty are visible
Lifecycle controls	release gate, rollback path, monitoring signal, incident threshold, refresh trigger, and model-card update owner	retention rule, access boundary, update cadence, deletion path, stewardship handoff, and dataset-card revision trigger	reuse is blocked without owner, retention, monitoring, rollback, and refresh evidence

Transparency notice:

Step	Artifact	Review gate
Public purpose	plain-language purpose, authority, affected service, and decision role	reader can tell why the system exists and where human judgment remains
Tool and data summary	model, data, supplier, provenance, validation, and accessibility summary	sensitive details are de-sensitized without hiding accountability fields
Impact and review	benefits, risks, safeguards, human review, appeal, and contact point	affected groups can identify recourse and oversight owners
Publication decision	publish, partially publish, delay, or hold decision with exemption rationale	non-public fields have a documented legal, security, privacy, or IP basis

Records retention and audit trail:

Record	Retained fields	Audit question
Source and prompt register	source identity, prompt version, tool allowlist, reviewer, timestamp, and caveat	Can a later reviewer reconstruct the evidentiary path without private or live data?
Decision and exception log	risk owner, accepted exception, compensating control, expiry date, and approval	Is every deviation time-bound, justified, and reviewable?
Artifact retention note	output type, sensitivity, access boundary, deletion rule, and refresh trigger	Does the retention choice match the educational purpose and rights impact?
Incident and remediation record	incident signal, containment action, root cause, owner, retest result, and closure date	Can the same failure be detected and prevented in the next reuse cycle?

Release and change-control gate:

Gate	Release evidence	Block condition
Scope freeze	accountable use case, excluded actions, tool profile, and data boundary	scope expands to external action, live data, or an unreviewed capability
Security and rights review	privacy, accessibility, security, bias, and human-review checks	rights impact, vulnerability, or accessibility issue has no owner
Version and rollback	model or prompt version, changelog, test fixture, and rollback path	change cannot be reproduced, compared, or reverted
Post-release monitoring	monitoring signal, incident threshold, refresh trigger, and owner	deployment or reuse occurs without logging and retest commitments

Risk exception memo:

Field	Minimum content	Approval rule
Exception requested	what requirement cannot be met, why, affected groups, and duration	exception must be specific, time-bound, and tied to a compensating control
Risk basis	likelihood, impact, evidence, uncertainty, alternatives, and rejected options	unsupported confidence or missing alternatives returns the memo for revision
Compensating control	human review, monitoring, access limit, disclosure, remediation, and owner	control must reduce risk without creating an operational workaround
Expiry and retest	expiry date, retest condition, review cadence, and closure criteria	open-ended exceptions are rejected

Learner support and accommodation plan:

Need	Support	Evidence
Access and modality	captions, alt text, keyboard path, plain-language summary, and structured tables	accessibility checklist, defect log, and retest result
Cognitive load	worked examples, staged release, glossary, checklist, and optional practice fixture	UDL design note and learner feedback record
Assessment fairness	allowed-tool statement, AI-use declaration, alternative submission mode, and transparent rubric	assessment-integrity note and accommodation record
Feedback and remediation	revision path, office-hour prompt, example correction, and due-date flexibility policy	feedback log and instructor disposition

Instructor question bank:

Question type	Prompt	Evidence
Source challenge	Which claim would fail if the strongest source were removed or downgraded?	claim ledger revision and source-lane note
Boundary challenge	Where could this exercise drift from analysis into action, and what safe substitute prevents it?	safe-substitution decision and excluded-action card
Rights challenge	Which affected group, accessibility need, privacy interest, or redress path is under-specified?	HRIA/DPIA update and accommodation note
Assurance challenge	What failure would the current evaluation miss, and what retest would reveal it?	adversarial assurance retest and remediation owner

Remediation backlog:

Backlog item	Trigger	Closure evidence
Unverified claim	claim lacks a guide citation or directly verified anchor	verified source, removed claim, or explicit source-guide context note
Unsafe phrasing	wording implies live targeting, external action, exploitation, manipulation, or unsafe control	safe substitute, blocked context, and reviewer sign-off
Accessibility defect	artifact cannot be inspected through an expected assistive or alternative workflow	defect fix, alternative means, and retest result
Assurance gap	evaluation, release, exception, incident, or vendor evidence is incomplete	owner, due date, retest, and accepted disposition

74.1.9 AutoGen and MCP Patterns rubric scoring bands

Section anchor. Section 74.

Band	Evidence standard	Disposition
4 - ready	source identity, accessibility, rights, safety, and reviewer evidence are complete	may be reused after normal refresh review
3 - revise	one evidence field is incomplete but risk is bounded and remediable	revise before reuse
2 - hold	multiple evidence fields are incomplete or ownership is unclear	hold for instructor and assurance review
1 - reject	unsafe action, private data, inaccessible artifact, or unverified claim appears	reject and rebuild from safe inputs

74.1.10 AutoGen and MCP Patterns refresh evidence

Section anchor. Section 74.

Evidence item	Refresh trigger	Retained support
Source lane	official source, standard, or legal text changes	checked-as-of date and source note
Safety treatment	operational wording or unsafe motif appears	safe-substitution decision and blocked context
Accessibility	WCAG, UDL, or institutional accessibility duty changes	defect log, retest result, and owner
Rights	privacy, human-rights, public transparency, or education guidance changes	HRIA/DPIA revision note
Vendor/tool	contract, data-use, incident, or model capability changes	procurement packet and incident review

74.1.11 AutoGen and MCP Patterns validation rubric

Section anchor. Section 74.

Criterion	Passing evidence
Source identity	existing `ageintNNN` keys remain stable or new references are append-only
Verification	official, standards, public-domain, or scholarly URL is checked directly
Safety	method is converted into tabletop, audit, governance, or synthetic-data treatment
Reproducibility	another reviewer can rebuild the artifact from retained inputs
Rights review	privacy, IP, human-rights, workforce, and education impacts are considered where relevant

74.1.12 AutoGen and MCP Patterns debrief protocol and reuse decision

Section anchor. Section 74.

Debrief by naming what the artifact can support, what it does not establish, what source changed, what risk was avoided by safe substitution, what human approval is still required, and when the appendix should be refreshed for AutoGen Code-Execution Exploit Chain (with Sandboxing Countermeasure); MCP Server: Building a STIX/TAXII Intelligence Tool Server.

74.2 MCP and AutoGen source boundary

This appendix separates protocol claims, framework-pattern claims, and security claims before learners build any classroom artifact. MCP interoperability language is grounded in the version-pinned official specification; tool-consent, confused-deputy, token-handling, and least-privilege language is grounded in the official MCP security guidance and NSA security-design guidance. STIX/TAXII examples are treated as standards-governed data-exchange examples, not as permission to connect to external systems [Project, 2025c]; [Project, 2025b]; [Agency, 2026i]; [Committee, 2025]; [Committee, 2021].

AutoGen and multi-agent framework rows remain a safe-substitution exercise: the learner may compare orchestration patterns, sandbox policies, denied-action logs, and reviewer evidence, but may not run external code, contact live services, or treat framework names as assurance evidence. When the source guide supplies only framework or security context, this appendix records the limitation and routes normative claims back to the official protocol, standards, and security anchors rather than laundering them through an agent-generated summary [147, 2026]; [153, 2026]; [155, 2026]; [299, 2026]; [309, 2026]; [310, 2026].

74.2.1 AutoGen and MCP Patterns visual navigation and evidence figures: purpose, source flow, and limits

The appendix uses Figure 150, Figure 151, and Figure 10 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.

Navigation links: Section 2, Section 73, Section 75.

74.2.2 AutoGen and MCP Patterns runtime item map and source roster: generated rows and citation support

Safe curriculum treatment	Blocked source motif, audit-only	Allowed fixture	Rejected action	Required artifact	Citation spine
AutoGen sandbox and code-execution approval review	D.1 retained for audit; operational wording transformed	toy OSINT fixtures, sandbox policy cards, and blocked-action logs	external execution, credentialed access, network calls, or unmanaged tool use	tool-isolation run card and denied-action evidence	-
D.2 MCP Server: Building a STIX/TAXII Intelligence Tool Server	no blocked motif; source title used verbatim	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	-
D.3 MCP Security: NSA Guidance Implementation in Python	no blocked motif; source title used verbatim	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	[155, 2026]
D.4 AutoGen GroupChat for Competing Hypothesis Analysis	no blocked motif; source title used verbatim	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	-

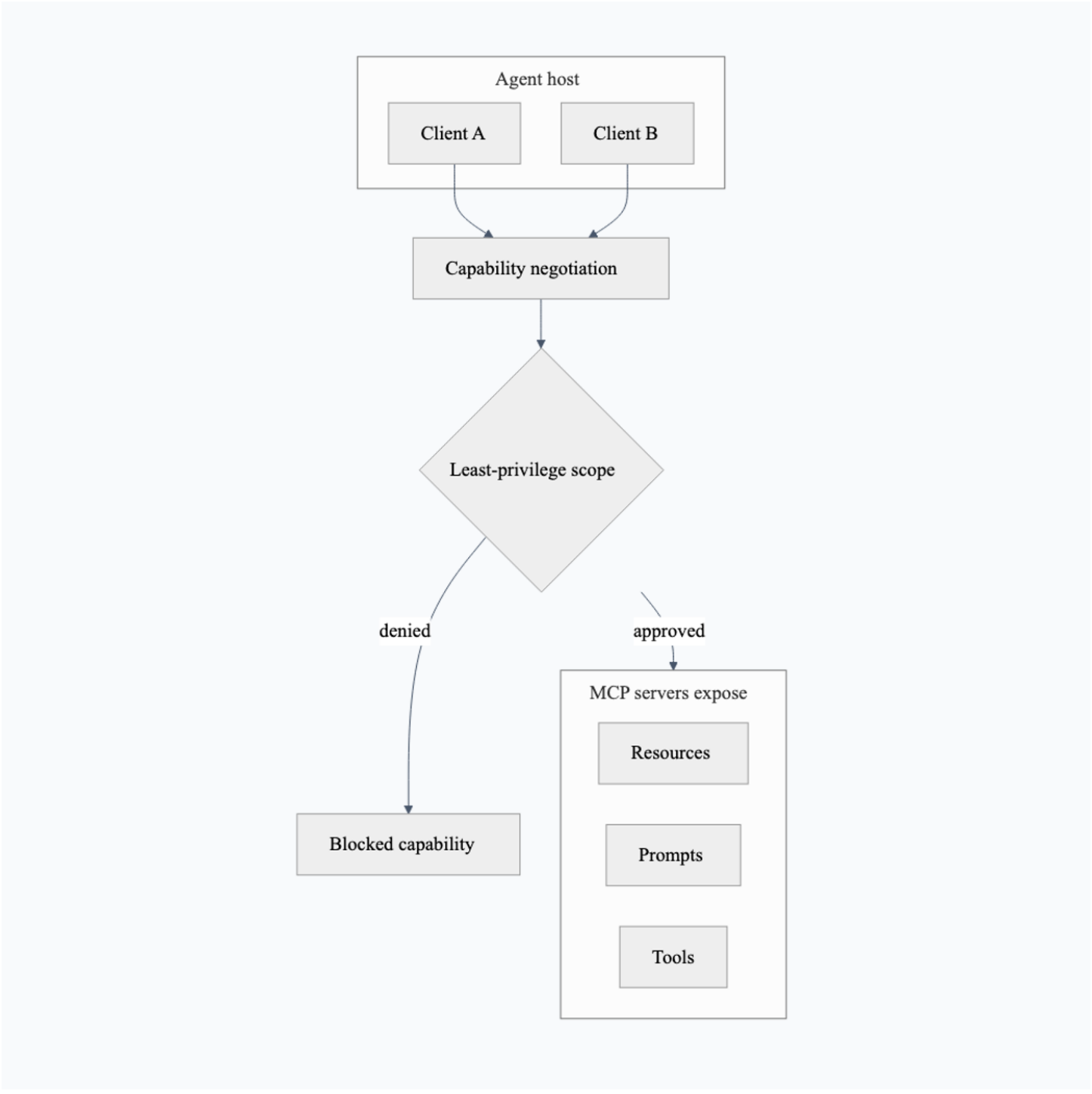


Figure 150: MCP standardizes how an agent host connects through clients to servers that expose resources, prompts, and tools under capability negotiation and least-privilege scoping. In the autogen and mcp patterns appendix, it lets readers compare Agent host, Client A, Client B, and Capability negotiation so the visual functions as a traceable course aid rather than an unscoped assertion.

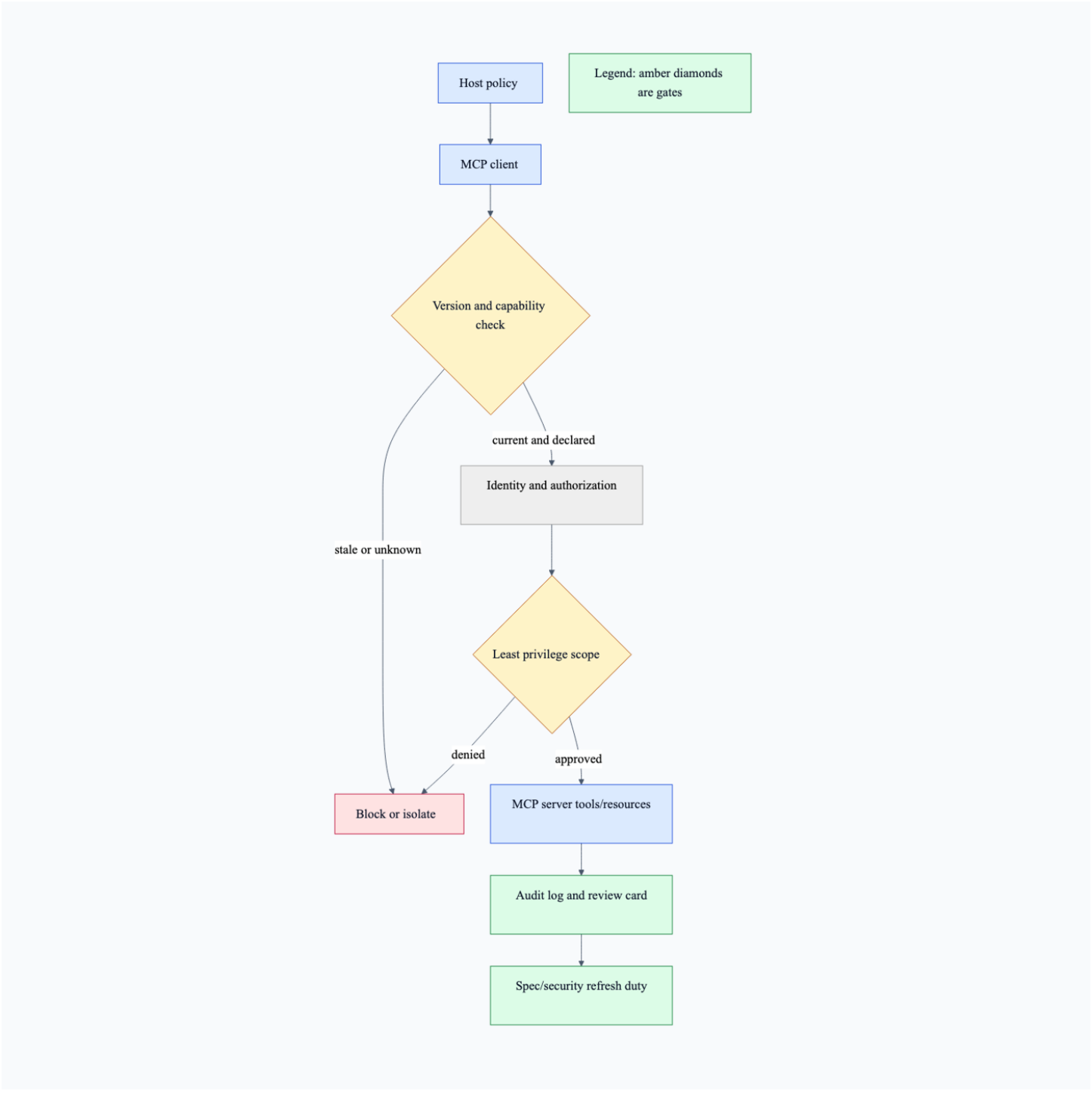


Figure 151: Conceptual schematic showing that MCP tool access depends on host, client, server, version, identity, authorization, and audit evidence rather than protocol names alone. In the autogen and mcp patterns appendix, it lets readers compare Host policy, MCP client, Identity and authorization, and Block or isolate so the visual functions as a traceable course aid rather than an unscoped assertion.

75 Cryptographic Methods

The current appendix is an evidence workbook for reusable classroom methods. It is educational and evidence-bounded: examples remain synthetic, defensive, lawful, and bounded to owned labs, public sources, or tabletop exercises. Source-item focus: One-Time Pad: Theory and Python Implementation; Signal Protocol and Modern E2E Encryption Architecture.

75.1 Cryptographic Methods workbook scope: purpose, safety envelope, and reuse decision

Section anchor. Section 75.

75.1.1 Cryptographic Methods operating purpose

Section anchor. Section 75.

The current appendix supports a reusable methods workbook. Each source item is treated as a reviewable classroom artifact rather than an operational instruction; examples begin with One-Time Pad: Theory and Python Implementation; Signal Protocol and Modern E2E Encryption Architecture.

75.1.2 Cryptographic Methods allowed-input boundary

Section anchor. Section 75.

Allowed inputs for the current appendix are public official or scholarly sources, standards text, instructor-provided excerpts, synthetic datasets, owned-lab logs, toy examples, and generated rubrics that expose their provenance for One-Time Pad: Theory and Python Implementation; Signal Protocol and Modern E2E Encryption Architecture.

75.1.3 Cryptographic Methods excluded-action boundary

Section anchor. Section 75.

Excluded actions for the current appendix are unauthorized collection, private-data processing, credential use, contact with real targets, live system interaction, exploit execution, deception, unsafe cyber-physical action, or external deployment while handling One-Time Pad: Theory and Python Implementation; Signal Protocol and Modern E2E Encryption Architecture.

75.1.4 Cryptographic Methods expected artifact package

Section anchor. Section 75.

Expected appendix artifacts are a purpose statement, allowed-inputs card, excluded-actions card, source-lane map, provenance record, claim ledger, safe-substitution note, output schema, review rubric, and capstone handoff memo for One-Time Pad: Theory and Python Implementation; Signal Protocol and Modern E2E Encryption Architecture.

75.1.5 Cryptographic Methods safe artifact schema

Section anchor. Section 75.

Field	Required evidence	Reject condition
Purpose	lawful educational, governance, research, or defensive purpose	vague operational objective or missing authority
Inputs	public, official, scholarly, synthetic, owned-lab, or instructor-provided material	private data, live target data, credentialed access, or unclear provenance
Transform	summary, comparison, rubric scoring, tabletop simulation, or audit review	collection expansion, external action, or unsafe system interaction
Output	memo, matrix, checklist, ledger, rubric, or debrief packet	deployable procedure, target package, or automated action plan
Reviewer	human reviewer, approval gate, revision note, and refresh owner	anonymous ownership or no escalation path

75.1.6 Cryptographic Methods input/output contract

Section anchor. Section 75.

Contract term	Input rule	Output rule
Source identity	retain `ageintNNN`, title, URL, and checked status	cite with Pandoc keys and avoid pasted raw URLs in prose
Accessibility	include plain-language labels, table headers, and figure alternatives	reject inaccessible figures, unlabeled tables, or single-modality evidence
Rights	identify affected groups, safeguards, and residual risk	preserve privacy, equality, access, contestability, and redress notes
Tooling	use allowlisted tools, visible prompts, logs, and stop conditions	keep outputs evidence-bounded, reversible, and human-reviewed
Refresh	record source, policy, standard, incident, or assessment trigger	assign an owner and date for revalidation

75.1.7 Cryptographic Methods failure cases and required responses

Section anchor. Section 75.

Failure case	Signal	Required response
Source laundering	claim cites an agent summary instead of a verified source	rebuild the claim ledger from direct sources
Boundary drift	exercise starts asking for live targets, private data, or external action	stop, substitute synthetic inputs, and document the block
Accessibility gap	learner cannot inspect, navigate, or complete the artifact	remediate and retest before reuse
Rights gap	affected group, safeguard, or redress path is missing	run HRIA/DPIA worksheet and escalate unresolved risk

Failure case	Signal	Required response
Vendor opacity	tool owner, data use, logs, or exit path is unknown	replace tool or pause until procurement evidence exists

75.1.8 Cryptographic Methods evidence package schemas

Section anchor. Section 75.

Model and dataset card:

Field	Model card evidence	Dataset card evidence	Review gate
Intended use	accountable task, excluded uses, affected users, human reviewer, and accountable owner	Data Cards purpose statement, recommended use, prohibited reuse, stewardship owner, and affected stakeholder groups	claim is rejected if intended use, excluded use, affected users, or owner is missing
Provenance and collection	model family, version, supplier or lab, training cutoff, deployment context, and configuration hash	upstream source, collection process, annotation method, consent or authority basis, sensitivity class, and license	artifact is held if provenance, license, authority, or collection process is opaque
Composition and limits	capability boundary, known failure modes, tool permissions, context window limits, and unsupported conditions	population, sampling frame, coverage gaps, subgroup visibility, missingness, transformations, and known caveats	artifact is revised if population, coverage, or source limits are invisible
Evaluation and caveats	benchmark suite, task-specific tests, subgroup or context results, red-team findings, uncertainty notes, and failure examples	quality tests, label agreement, bias review, measurement limits, transformation log, and Data Cards answer-evaluation notes	empirical or performance claims are rejected unless test context, subgroup caveats, and uncertainty are visible
Lifecycle controls	release gate, rollback path, monitoring signal, incident threshold, refresh trigger, and model-card update owner	retention rule, access boundary, update cadence, deletion path, stewardship handoff, and dataset-card revision trigger	reuse is blocked without owner, retention, monitoring, rollback, and refresh evidence

Transparency notice:

Step	Artifact	Review gate
Public purpose	plain-language purpose, authority, affected service, and decision role	reader can tell why the system exists and where human judgment remains
Tool and data summary	model, data, supplier, provenance, validation, and accessibility summary	sensitive details are de-sensitized without hiding accountability fields
Impact and review	benefits, risks, safeguards, human review, appeal, and contact point	affected groups can identify recourse and oversight owners
Publication decision	publish, partially publish, delay, or hold decision with exemption rationale	non-public fields have a documented legal, security, privacy, or IP basis

Records retention and audit trail:

Record	Retained fields	Audit question
Source and prompt register	source identity, prompt version, tool allowlist, reviewer, timestamp, and caveat	Can a later reviewer reconstruct the evidentiary path without private or live data?
Decision and exception log	risk owner, accepted exception, compensating control, expiry date, and approval	Is every deviation time-bound, justified, and reviewable?
Artifact retention note	output type, sensitivity, access boundary, deletion rule, and refresh trigger	Does the retention choice match the educational purpose and rights impact?
Incident and remediation record	incident signal, containment action, root cause, owner, retest result, and closure date	Can the same failure be detected and prevented in the next reuse cycle?

Release and change-control gate:

Gate	Release evidence	Block condition
Scope freeze	accountable use case, excluded actions, tool profile, and data boundary	scope expands to external action, live data, or an unreviewed capability
Security and rights review	privacy, accessibility, security, bias, and human-review checks	rights impact, vulnerability, or accessibility issue has no owner
Version and rollback	model or prompt version, changelog, test fixture, and rollback path	change cannot be reproduced, compared, or reverted
Post-release monitoring	monitoring signal, incident threshold, refresh trigger, and owner	deployment or reuse occurs without logging and retest commitments

Risk exception memo:

Field	Minimum content	Approval rule
Exception requested	what requirement cannot be met, why, affected groups, and duration	exception must be specific, time-bound, and tied to a compensating control
Risk basis	likelihood, impact, evidence, uncertainty, alternatives, and rejected options	unsupported confidence or missing alternatives returns the memo for revision
Compensating control	human review, monitoring, access limit, disclosure, remediation, and owner	control must reduce risk without creating an operational workaround
Expiry and retest	expiry date, retest condition, review cadence, and closure criteria	open-ended exceptions are rejected

Learner support and accommodation plan:

Need	Support	Evidence
Access and modality	captions, alt text, keyboard path, plain-language summary, and structured tables	accessibility checklist, defect log, and retest result
Cognitive load	worked examples, staged release, glossary, checklist, and optional practice fixture	UDL design note and learner feedback record
Assessment fairness	allowed-tool statement, AI-use declaration, alternative submission mode, and transparent rubric	assessment-integrity note and accommodation record
Feedback and remediation	revision path, office-hour prompt, example correction, and due-date flexibility policy	feedback log and instructor disposition

Instructor question bank:

Question type	Prompt	Evidence
Source challenge	Which claim would fail if the strongest source were removed or downgraded?	claim ledger revision and source-lane note
Boundary challenge	Where could this exercise drift from analysis into action, and what safe substitute prevents it?	safe-substitution decision and excluded-action card
Rights challenge	Which affected group, accessibility need, privacy interest, or redress path is under-specified?	HRIA/DPIA update and accommodation note
Assurance challenge	What failure would the current evaluation miss, and what retest would reveal it?	adversarial assurance retest and remediation owner

Remediation backlog:

Backlog item	Trigger	Closure evidence
Unverified claim	claim lacks a guide citation or directly verified anchor	verified source, removed claim, or explicit source-guide context note
Unsafe phrasing	wording implies live targeting, external action, exploitation, manipulation, or unsafe control	safe substitute, blocked context, and reviewer sign-off
Accessibility defect	artifact cannot be inspected through an expected assistive or alternative workflow	defect fix, alternative means, and retest result
Assurance gap	evaluation, release, exception, incident, or vendor evidence is incomplete	owner, due date, retest, and accepted disposition

75.1.9 Cryptographic Methods rubric scoring bands

Section anchor. Section 75.

Band	Evidence standard	Disposition
4 - ready	source identity, accessibility, rights, safety, and reviewer evidence are complete	may be reused after normal refresh review
3 - revise	one evidence field is incomplete but risk is bounded and remediable	revise before reuse
2 - hold	multiple evidence fields are incomplete or ownership is unclear	hold for instructor and assurance review
1 - reject	unsafe action, private data, inaccessible artifact, or unverified claim appears	reject and rebuild from safe inputs

75.1.10 Cryptographic Methods refresh evidence

Section anchor. Section 75.

Evidence item	Refresh trigger	Retained support
Source lane	official source, standard, or legal text changes	checked-as-of date and source note
Safety treatment	operational wording or unsafe motif appears	safe-substitution decision and blocked context
Accessibility	WCAG, UDL, or institutional accessibility duty changes	defect log, retest result, and owner
Rights	privacy, human-rights, public transparency, or education guidance changes	HRIA/DPIA revision note
Vendor/tool	contract, data-use, incident, or model capability changes	procurement packet and incident review

75.1.11 Cryptographic Methods validation rubric

Section anchor. Section 75.

Criterion	Passing evidence
Source identity	existing `ageintNNN` keys remain stable or new references are append-only
Verification	official, standards, public-domain, or scholarly URL is checked directly
Safety	method is converted into tabletop, audit, governance, or synthetic-data treatment
Reproducibility	another reviewer can rebuild the artifact from retained inputs
Rights review	privacy, IP, human-rights, workforce, and education impacts are considered where relevant

75.1.12 Cryptographic Methods debrief protocol and reuse decision

Section anchor. Section 75.

Debrief by naming what the artifact can support, what it does not establish, what source changed, what risk was avoided by safe substitution, what human approval is still required, and when the appendix should be refreshed for One-Time Pad: Theory and Python Implementation; Signal Protocol and Modern E2E Encryption Architecture.

75.2 Cryptographic standards boundary

This appendix treats cryptography as an assurance and governance subject. Confidentiality, hashing, digital signatures, and key management are grounded in NIST standards and lifecycle guidance; classroom work may inspect properties, terminology, and review evidence, but it must not become operational secrecy, covert communications, evasion, or live key-management instruction [of Standards and , NIST]; [of Standards and , NIST]; [of Standards and , NIST]; [, NIST].

The source-guide material on dead drops and steganography is retained only as historical or detection-literacy context. A learner-facing artifact should map claim type to evidence type: standards for cryptographic properties, scholarly or official sources for evaluation claims, and explicit blocked-use notes for anything that could drift toward covert channels or uncontrolled deployment [027, 2026]; [028, 2026]; Figure 152.

75.2.1 Cryptographic Methods visual navigation and evidence figures: purpose, source flow, and limits

The appendix uses Figure 152 and Figure 10 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.

Navigation links: Section 2, Section 74, Section 76.

75.2.2 Cryptographic Methods runtime item map and source roster: generated rows and citation support

Safe curriculum treatment	Blocked source motif, audit-only	Allowed fixture	Rejected action	Required artifact	Citation spine
E.1 One-Time Pad: Theory and Python Implementation	no blocked motif; source title used verbatim	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	-
E.2 Signal Protocol and Modern E2E Encryption Architecture	no blocked motif; source title used verbatim	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	-
E.3 PGP/GPG for Operational Security: Key Management	no blocked motif; source title used verbatim	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	-
Steganography detection-literacy and communications-security review	E.4 retained for audit; operational wording transformed	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	[028, 2026]
E.5 Digital Dead Drop Implementation: Email/PasteBin/S3	no blocked motif; source title used verbatim	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	-

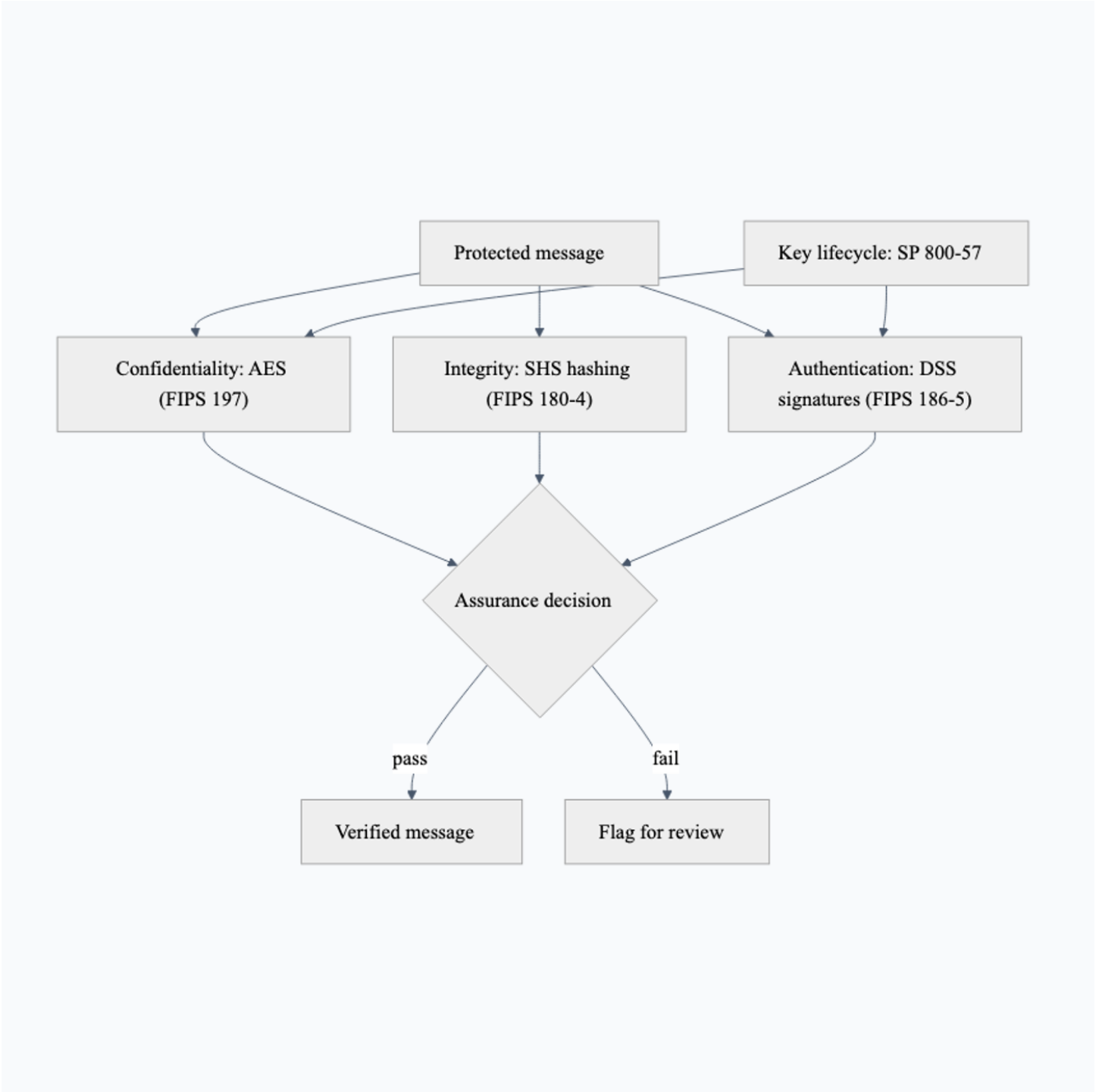


Figure 152: The cryptographic methods appendix maps each standard to the assurance property it provides, from confidentiality and integrity to authentication and key lifecycle governance. Its reader value is to make Protected message, Confidentiality: AES (FIPS 197), Integrity: SHS hashing (FIPS 180-4), and Authentication: DSS signatures (FIPS 186-5) visible at a glance, with the cryptographic methods appendix as the source section and defensive review as the boundary.

76 ATT&CK and Kill Chain Mapping Templates

The current appendix is an evidence workbook for reusable classroom methods. It is educational and evidence-bounded: examples remain synthetic, defensive, lawful, and bounded to owned labs, public sources, or tabletop exercises. Source-item focus: MITRE ATT&CK Navigator Layer: Enterprise; the module Navigator Layer.

76.1 ATT&CK and Kill Chain Mapping Templates workbook scope: purpose, safety envelope, and reuse decision

Section anchor. Section 76.

76.1.1 ATT&CK and Kill Chain Mapping Templates operating purpose

Section anchor. Section 76.

The current appendix supports a reusable methods workbook. Each source item is treated as a reviewable classroom artifact rather than an operational instruction; examples begin with MITRE ATT&CK Navigator Layer: Enterprise; the module Navigator Layer.

76.1.2 ATT&CK and Kill Chain Mapping Templates allowed-input boundary

Section anchor. Section 76.

Allowed inputs for the current appendix are public official or scholarly sources, standards text, instructor-provided excerpts, synthetic datasets, owned-lab logs, toy examples, and generated rubrics that expose their provenance for MITRE ATT&CK Navigator Layer: Enterprise; the module Navigator Layer.

76.1.3 ATT&CK and Kill Chain Mapping Templates excluded-action boundary

Section anchor. Section 76.

Excluded actions for the current appendix are unauthorized collection, private-data processing, credential use, contact with real targets, live system interaction, exploit execution, deception, unsafe cyber-physical action, or external deployment while handling MITRE ATT&CK Navigator Layer: Enterprise; the module Navigator Layer.

76.1.4 ATT&CK and Kill Chain Mapping Templates expected artifact package

Section anchor. Section 76.

Expected appendix artifacts are a purpose statement, allowed-inputs card, excluded-actions card, source-lane map, provenance record, claim ledger, safe-substitution note, output schema, review rubric, and capstone handoff memo for MITRE ATT&CK Navigator Layer: Enterprise; the module Navigator Layer.

76.1.5 ATT&CK and Kill Chain Mapping Templates safe artifact schema

Section anchor. Section 76.

Field	Required evidence	Reject condition
Purpose	lawful educational, governance, research, or defensive purpose	vague operational objective or missing authority
Inputs	public, official, scholarly, synthetic, owned-lab, or instructor-provided material	private data, live target data, credentialed access, or unclear provenance
Transform	summary, comparison, rubric scoring, tabletop simulation, or audit review	collection expansion, external action, or unsafe system interaction
Output	memo, matrix, checklist, ledger, rubric, or debrief packet	deployable procedure, target package, or automated action plan
Reviewer	human reviewer, approval gate, revision note, and refresh owner	anonymous ownership or no escalation path

76.1.6 ATT&CK and Kill Chain Mapping Templates input/output contract

Section anchor. Section 76.

Contract term	Input rule	Output rule
Source identity	retain `ageintNNN`, title, URL, and checked status	cite with Pandoc keys and avoid pasted raw URLs in prose
Accessibility	include plain-language labels, table headers, and figure alternatives	reject inaccessible figures, unlabeled tables, or single-modality evidence
Rights	identify affected groups, safeguards, and residual risk	preserve privacy, equality, access, contestability, and redress notes
Tooling	use allowlisted tools, visible prompts, logs, and stop conditions	keep outputs evidence-bounded, reversible, and human-reviewed
Refresh	record source, policy, standard, incident, or assessment trigger	assign an owner and date for revalidation

76.1.7 ATT&CK and Kill Chain Mapping Templates failure cases and required responses

Section anchor. Section 76.

Failure case	Signal	Required response
Source laundering	claim cites an agent summary instead of a verified source	rebuild the claim ledger from direct sources
Boundary drift	exercise starts asking for live targets, private data, or external action	stop, substitute synthetic inputs, and document the block
Accessibility gap	learner cannot inspect, navigate, or complete the artifact	remediate and retest before reuse
Rights gap	affected group, safeguard, or redress path is missing	run HRIA/DPIA worksheet and escalate unresolved risk

Failure case	Signal	Required response
Vendor opacity	tool owner, data use, logs, or exit path is unknown	replace tool or pause until procurement evidence exists

76.1.8 ATT&CK and Kill Chain Mapping Templates evidence package schemas

Section anchor. Section 76.

Model and dataset card:

Field	Model card evidence	Dataset card evidence	Review gate
Intended use	accountable task, excluded uses, affected users, human reviewer, and accountable owner	Data Cards purpose statement, recommended use, prohibited reuse, stewardship owner, and affected stakeholder groups	claim is rejected if intended use, excluded use, affected users, or owner is missing
Provenance and collection	model family, version, supplier or lab, training cutoff, deployment context, and configuration hash	upstream source, collection process, annotation method, consent or authority basis, sensitivity class, and license	artifact is held if provenance, license, authority, or collection process is opaque
Composition and limits	capability boundary, known failure modes, tool permissions, context window limits, and unsupported conditions	population, sampling frame, coverage gaps, subgroup visibility, missingness, transformations, and known caveats	artifact is revised if population, coverage, or source limits are invisible
Evaluation and caveats	benchmark suite, task-specific tests, subgroup or context results, red-team findings, uncertainty notes, and failure examples	quality tests, label agreement, bias review, measurement limits, transformation log, and Data Cards answer-evaluation notes	empirical or performance claims are rejected unless test context, subgroup caveats, and uncertainty are visible
Lifecycle controls	release gate, rollback path, monitoring signal, incident threshold, refresh trigger, and model-card update owner	retention rule, access boundary, update cadence, deletion path, stewardship handoff, and dataset-card revision trigger	reuse is blocked without owner, retention, monitoring, rollback, and refresh evidence

Transparency notice:

Step	Artifact	Review gate
Public purpose	plain-language purpose, authority, affected service, and decision role	reader can tell why the system exists and where human judgment remains
Tool and data summary	model, data, supplier, provenance, validation, and accessibility summary	sensitive details are de-sensitized without hiding accountability fields
Impact and review	benefits, risks, safeguards, human review, appeal, and contact point	affected groups can identify recourse and oversight owners
Publication decision	publish, partially publish, delay, or hold decision with exemption rationale	non-public fields have a documented legal, security, privacy, or IP basis

Records retention and audit trail:

Record	Retained fields	Audit question
Source and prompt register	source identity, prompt version, tool allowlist, reviewer, timestamp, and caveat	Can a later reviewer reconstruct the evidentiary path without private or live data?
Decision and exception log	risk owner, accepted exception, compensating control, expiry date, and approval	Is every deviation time-bound, justified, and reviewable?
Artifact retention note	output type, sensitivity, access boundary, deletion rule, and refresh trigger	Does the retention choice match the educational purpose and rights impact?
Incident and remediation record	incident signal, containment action, root cause, owner, retest result, and closure date	Can the same failure be detected and prevented in the next reuse cycle?

Release and change-control gate:

Gate	Release evidence	Block condition
Scope freeze	accountable use case, excluded actions, tool profile, and data boundary	scope expands to external action, live data, or an unreviewed capability
Security and rights review	privacy, accessibility, security, bias, and human-review checks	rights impact, vulnerability, or accessibility issue has no owner
Version and rollback	model or prompt version, changelog, test fixture, and rollback path	change cannot be reproduced, compared, or reverted
Post-release monitoring	monitoring signal, incident threshold, refresh trigger, and owner	deployment or reuse occurs without logging and retest commitments

Risk exception memo:

Field	Minimum content	Approval rule
Exception requested	what requirement cannot be met, why, affected groups, and duration	exception must be specific, time-bound, and tied to a compensating control
Risk basis	likelihood, impact, evidence, uncertainty, alternatives, and rejected options	unsupported confidence or missing alternatives returns the memo for revision
Compensating control	human review, monitoring, access limit, disclosure, remediation, and owner	control must reduce risk without creating an operational workaround
Expiry and retest	expiry date, retest condition, review cadence, and closure criteria	open-ended exceptions are rejected

Learner support and accommodation plan:

Need	Support	Evidence
Access and modality	captions, alt text, keyboard path, plain-language summary, and structured tables	accessibility checklist, defect log, and retest result
Cognitive load	worked examples, staged release, glossary, checklist, and optional practice fixture	UDL design note and learner feedback record
Assessment fairness	allowed-tool statement, AI-use declaration, alternative submission mode, and transparent rubric	assessment-integrity note and accommodation record
Feedback and remediation	revision path, office-hour prompt, example correction, and due-date flexibility policy	feedback log and instructor disposition

Instructor question bank:

Question type	Prompt	Evidence
Source challenge	Which claim would fail if the strongest source were removed or downgraded?	claim ledger revision and source-lane note
Boundary challenge	Where could this exercise drift from analysis into action, and what safe substitute prevents it?	safe-substitution decision and excluded-action card
Rights challenge	Which affected group, accessibility need, privacy interest, or redress path is under-specified?	HRIA/DPIA update and accommodation note
Assurance challenge	What failure would the current evaluation miss, and what retest would reveal it?	adversarial assurance retest and remediation owner

Remediation backlog:

Backlog item	Trigger	Closure evidence
Unverified claim	claim lacks a guide citation or directly verified anchor	verified source, removed claim, or explicit source-guide context note
Unsafe phrasing	wording implies live targeting, external action, exploitation, manipulation, or unsafe control	safe substitute, blocked context, and reviewer sign-off
Accessibility defect	artifact cannot be inspected through an expected assistive or alternative workflow	defect fix, alternative means, and retest result
Assurance gap	evaluation, release, exception, incident, or vendor evidence is incomplete	owner, due date, retest, and accepted disposition

76.1.9 ATT&CK and Kill Chain Mapping Templates rubric scoring bands

Section anchor. Section 76.

Band	Evidence standard	Disposition
4 - ready	source identity, accessibility, rights, safety, and reviewer evidence are complete	may be reused after normal refresh review
3 - revise	one evidence field is incomplete but risk is bounded and remediable	revise before reuse
2 - hold	multiple evidence fields are incomplete or ownership is unclear	hold for instructor and assurance review
1 - reject	unsafe action, private data, inaccessible artifact, or unverified claim appears	reject and rebuild from safe inputs

76.1.10 ATT&CK and Kill Chain Mapping Templates refresh evidence

Section anchor. Section 76.

Evidence item	Refresh trigger	Retained support
Source lane	official source, standard, or legal text changes	checked-as-of date and source note
Safety treatment	operational wording or unsafe motif appears	safe-substitution decision and blocked context
Accessibility	WCAG, UDL, or institutional accessibility duty changes	defect log, retest result, and owner
Rights	privacy, human-rights, public transparency, or education guidance changes	HRIA/DPIA revision note
Vendor/tool	contract, data-use, incident, or model capability changes	procurement packet and incident review

76.1.11 ATT&CK and Kill Chain Mapping Templates validation rubric

Section anchor. Section 76.

Criterion	Passing evidence
Source identity	existing `ageintNNN` keys remain stable or new references are append-only
Verification	official, standards, public-domain, or scholarly URL is checked directly
Safety	method is converted into tabletop, audit, governance, or synthetic-data treatment
Reproducibility	another reviewer can rebuild the artifact from retained inputs
Rights review	privacy, IP, human-rights, workforce, and education impacts are considered where relevant

76.1.12 ATT&CK and Kill Chain Mapping Templates debrief protocol and reuse decision

Section anchor. Section 76.

Debrief by naming what the artifact can support, what it does not establish, what source changed, what risk was avoided by safe substitution, what human approval is still required, and when the appendix should be refreshed for MITRE ATT&CK Navigator Layer: Enterprise; the module Navigator Layer.

76.1.13 ATT&CK and Kill Chain Mapping Templates visual navigation and evidence figures: purpose, source flow, and limits

The appendix uses Figure 153 and Figure 10 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 75, Section 77.

76.1.14 ATT&CK and Kill Chain Mapping Templates runtime item map and source roster: generated rows and citation support

Safe curriculum treatment	Blocked source motif, audit-only	Allowed fixture	Rejected action	Required artifact	Citation spine
F.1 MITRE ATT&CK Navigator Layer: Enterprise	no blocked motif; source title used verbatim	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	[063, 2026]
F.2 MITRE ATT&CK for ICS Navigator Layer	no blocked motif; source title used verbatim	synthetic process logs, operator-decision cards, and safety stop rules	live device interaction, process manipulation, unsafe actuation, or plant operation	tabletop packet with asset, consequence, operator decision, and recovery evidence	[213, 2026]
F.3 Cyber Kill Chain Campaign Mapping Worksheet	no blocked motif; source title used verbatim	fabricated alerts, published defensive taxonomy labels, and debrief notes	scanning, exploitation, credential use, blocking, containment, or evasion	defensive coverage matrix and incident debrief	[061, 2026]
F.4 Adversary Emulation Plan Template	no blocked motif; source title used verbatim	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	-
F.5 Threat Intelligence Report Template (STIX v2.1 JSON)	no blocked motif; source title used verbatim	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	-

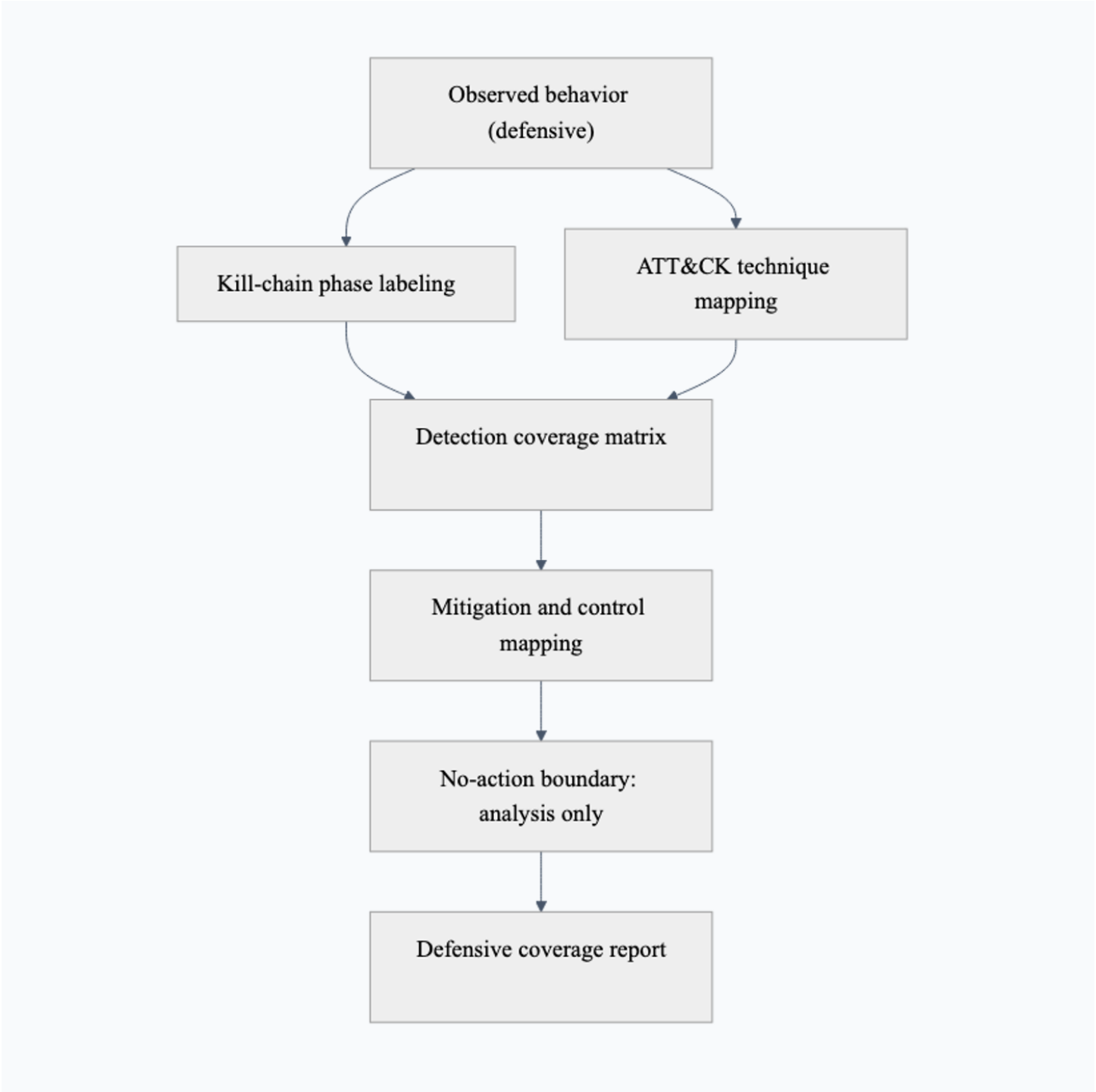


Figure 153: The mapping template aligns observed behaviors to kill-chain phases and ATT&CK techniques for defensive sequencing only, ending in detection coverage and mitigation, never an action plan. The captioned view belongs to the att ck and kill chain mapping templates appendix and should be read as a map of Observed behavior (defensive), Kill-chain phase labeling, ATT&CK technique mapping, and Detection coverage matrix, not as a capability score or live-task instruction.

77 Cognitive Security and Inoculation Methods

The current appendix is an evidence workbook for reusable classroom methods. It is educational and evidence-bounded: examples remain synthetic, defensive, lawful, and bounded to owned labs, public sources, or tabletop exercises. Source-item focus: CAMBREX Taxonomy of Manipulation Techniques (van der Linden); Python Prebunking Agent: Manipulation Detection + Inoculation Content Generation.

77.1 Cognitive Security and Inoculation Methods workbook scope: purpose, safety envelope, and reuse decision

Section anchor. Section 77.

77.1.1 Cognitive Security and Inoculation Methods operating purpose

Section anchor. Section 77.

The current appendix supports a reusable methods workbook. Each source item is treated as a reviewable classroom artifact rather than an operational instruction; examples begin with CAMBREX Taxonomy of Manipulation Techniques (van der Linden); Python Prebunking Agent: Manipulation Detection + Inoculation Content Generation.

77.1.2 Cognitive Security and Inoculation Methods allowed-input boundary

Section anchor. Section 77.

Allowed inputs for the current appendix are public official or scholarly sources, standards text, instructor-provided excerpts, synthetic datasets, owned-lab logs, toy examples, and generated rubrics that expose their provenance for CAMBREX Taxonomy of Manipulation Techniques (van der Linden); Python Prebunking Agent: Manipulation Detection + Inoculation Content Generation.

77.1.3 Cognitive Security and Inoculation Methods excluded-action boundary

Section anchor. Section 77.

Excluded actions for the current appendix are unauthorized collection, private-data processing, credential use, contact with real targets, live system interaction, exploit execution, deception, unsafe cyber-physical action, or external deployment while handling CAMBREX Taxonomy of Manipulation Techniques (van der Linden); Python Prebunking Agent: Manipulation Detection + Inoculation Content Generation.

77.1.4 Cognitive Security and Inoculation Methods expected artifact package

Section anchor. Section 77.

Expected appendix artifacts are a purpose statement, allowed-inputs card, excluded-actions card, source-lane map, provenance record, claim ledger, safe-substitution note, output schema, review rubric, and capstone handoff memo for CAMBREX Taxonomy of Manipulation Techniques (van der Linden); Python Prebunking Agent: Manipulation Detection + Inoculation Content Generation.

77.1.5 Cognitive Security and Inoculation Methods safe artifact schema

Section anchor. Section 77.

Field	Required evidence	Reject condition
Purpose	lawful educational, governance, research, or defensive purpose	vague operational objective or missing authority
Inputs	public, official, scholarly, synthetic, owned-lab, or instructor-provided material	private data, live target data, credentialed access, or unclear provenance
Transform	summary, comparison, rubric scoring, tabletop simulation, or audit review	collection expansion, external action, or unsafe system interaction
Output	memo, matrix, checklist, ledger, rubric, or debrief packet	deployable procedure, target package, or automated action plan
Reviewer	human reviewer, approval gate, revision note, and refresh owner	anonymous ownership or no escalation path

77.1.6 Cognitive Security and Inoculation Methods input/output contract

Section anchor. Section 77.

Contract term	Input rule	Output rule
Source identity	retain `ageintNNN`, title, URL, and checked status	cite with Pandoc keys and avoid pasted raw URLs in prose
Accessibility	include plain-language labels, table headers, and figure alternatives	reject inaccessible figures, unlabeled tables, or single-modality evidence
Rights	identify affected groups, safeguards, and residual risk	preserve privacy, equality, access, contestability, and redress notes
Tooling	use allowlisted tools, visible prompts, logs, and stop conditions	keep outputs evidence-bounded, reversible, and human-reviewed
Refresh	record source, policy, standard, incident, or assessment trigger	assign an owner and date for revalidation

77.1.7 Cognitive Security and Inoculation Methods failure cases and required responses

Section anchor. Section 77.

Failure case	Signal	Required response
Source laundering	claim cites an agent summary instead of a verified source	rebuild the claim ledger from direct sources
Boundary drift	exercise starts asking for live targets, private data, or external action	stop, substitute synthetic inputs, and document the block
Accessibility gap	learner cannot inspect, navigate, or complete the artifact	remediate and retest before reuse
Rights gap	affected group, safeguard, or redress path is missing	run HRIA/DPIA worksheet and escalate unresolved risk

Failure case	Signal	Required response
Vendor opacity	tool owner, data use, logs, or exit path is unknown	replace tool or pause until procurement evidence exists

77.1.8 Cognitive Security and Inoculation Methods evidence package schemas

Section anchor. Section 77.

Model and dataset card:

Field	Model card evidence	Dataset card evidence	Review gate
Intended use	accountable task, excluded uses, affected users, human reviewer, and accountable owner	Data Cards purpose statement, recommended use, prohibited reuse, stewardship owner, and affected stakeholder groups	claim is rejected if intended use, excluded use, affected users, or owner is missing
Provenance and collection	model family, version, supplier or lab, training cutoff, deployment context, and configuration hash	upstream source, collection process, annotation method, consent or authority basis, sensitivity class, and license	artifact is held if provenance, license, authority, or collection process is opaque
Composition and limits	capability boundary, known failure modes, tool permissions, context window limits, and unsupported conditions	population, sampling frame, coverage gaps, subgroup visibility, missingness, transformations, and known caveats	artifact is revised if population, coverage, or source limits are invisible
Evaluation and caveats	benchmark suite, task-specific tests, subgroup or context results, red-team findings, uncertainty notes, and failure examples	quality tests, label agreement, bias review, measurement limits, transformation log, and Data Cards answer-evaluation notes	empirical or performance claims are rejected unless test context, subgroup caveats, and uncertainty are visible
Lifecycle controls	release gate, rollback path, monitoring signal, incident threshold, refresh trigger, and model-card update owner	retention rule, access boundary, update cadence, deletion path, stewardship handoff, and dataset-card revision trigger	reuse is blocked without owner, retention, monitoring, rollback, and refresh evidence

Transparency notice:

Step	Artifact	Review gate
Public purpose	plain-language purpose, authority, affected service, and decision role	reader can tell why the system exists and where human judgment remains
Tool and data summary	model, data, supplier, provenance, validation, and accessibility summary	sensitive details are de-sensitized without hiding accountability fields
Impact and review	benefits, risks, safeguards, human review, appeal, and contact point	affected groups can identify recourse and oversight owners
Publication decision	publish, partially publish, delay, or hold decision with exemption rationale	non-public fields have a documented legal, security, privacy, or IP basis

Records retention and audit trail:

Record	Retained fields	Audit question
Source and prompt register	source identity, prompt version, tool allowlist, reviewer, timestamp, and caveat	Can a later reviewer reconstruct the evidentiary path without private or live data?
Decision and exception log	risk owner, accepted exception, compensating control, expiry date, and approval	Is every deviation time-bound, justified, and reviewable?
Artifact retention note	output type, sensitivity, access boundary, deletion rule, and refresh trigger	Does the retention choice match the educational purpose and rights impact?
Incident and remediation record	incident signal, containment action, root cause, owner, retest result, and closure date	Can the same failure be detected and prevented in the next reuse cycle?

Release and change-control gate:

Gate	Release evidence	Block condition
Scope freeze	accountable use case, excluded actions, tool profile, and data boundary	scope expands to external action, live data, or an unreviewed capability
Security and rights review	privacy, accessibility, security, bias, and human-review checks	rights impact, vulnerability, or accessibility issue has no owner
Version and rollback	model or prompt version, changelog, test fixture, and rollback path	change cannot be reproduced, compared, or reverted
Post-release monitoring	monitoring signal, incident threshold, refresh trigger, and owner	deployment or reuse occurs without logging and retest commitments

Risk exception memo:

Field	Minimum content	Approval rule
Exception requested	what requirement cannot be met, why, affected groups, and duration	exception must be specific, time-bound, and tied to a compensating control
Risk basis	likelihood, impact, evidence, uncertainty, alternatives, and rejected options	unsupported confidence or missing alternatives returns the memo for revision
Compensating control	human review, monitoring, access limit, disclosure, remediation, and owner	control must reduce risk without creating an operational workaround
Expiry and retest	expiry date, retest condition, review cadence, and closure criteria	open-ended exceptions are rejected

Learner support and accommodation plan:

Need	Support	Evidence
Access and modality	captions, alt text, keyboard path, plain-language summary, and structured tables	accessibility checklist, defect log, and retest result
Cognitive load	worked examples, staged release, glossary, checklist, and optional practice fixture	UDL design note and learner feedback record
Assessment fairness	allowed-tool statement, AI-use declaration, alternative submission mode, and transparent rubric	assessment-integrity note and accommodation record
Feedback and remediation	revision path, office-hour prompt, example correction, and due-date flexibility policy	feedback log and instructor disposition

Instructor question bank:

Question type	Prompt	Evidence
Source challenge	Which claim would fail if the strongest source were removed or downgraded?	claim ledger revision and source-lane note
Boundary challenge	Where could this exercise drift from analysis into action, and what safe substitute prevents it?	safe-substitution decision and excluded-action card
Rights challenge	Which affected group, accessibility need, privacy interest, or redress path is under-specified?	HRIA/DPIA update and accommodation note
Assurance challenge	What failure would the current evaluation miss, and what retest would reveal it?	adversarial assurance retest and remediation owner

Remediation backlog:

Backlog item	Trigger	Closure evidence
Unverified claim	claim lacks a guide citation or directly verified anchor	verified source, removed claim, or explicit source-guide context note
Unsafe phrasing	wording implies live targeting, external action, exploitation, manipulation, or unsafe control	safe substitute, blocked context, and reviewer sign-off
Accessibility defect	artifact cannot be inspected through an expected assistive or alternative workflow	defect fix, alternative means, and retest result
Assurance gap	evaluation, release, exception, incident, or vendor evidence is incomplete	owner, due date, retest, and accepted disposition

77.1.9 Cognitive Security and Inoculation Methods rubric scoring bands

Section anchor. Section 77.

Band	Evidence standard	Disposition
4 - ready	source identity, accessibility, rights, safety, and reviewer evidence are complete	may be reused after normal refresh review
3 - revise	one evidence field is incomplete but risk is bounded and remediable	revise before reuse
2 - hold	multiple evidence fields are incomplete or ownership is unclear	hold for instructor and assurance review
1 - reject	unsafe action, private data, inaccessible artifact, or unverified claim appears	reject and rebuild from safe inputs

77.1.10 Cognitive Security and Inoculation Methods refresh evidence

Section anchor. Section 77.

Evidence item	Refresh trigger	Retained support
Source lane	official source, standard, or legal text changes	checked-as-of date and source note
Safety treatment	operational wording or unsafe motif appears	safe-substitution decision and blocked context
Accessibility	WCAG, UDL, or institutional accessibility duty changes	defect log, retest result, and owner
Rights	privacy, human-rights, public transparency, or education guidance changes	HRIA/DPIA revision note
Vendor/tool	contract, data-use, incident, or model capability changes	procurement packet and incident review

77.1.11 Cognitive Security and Inoculation Methods validation rubric

Section anchor. Section 77.

Criterion	Passing evidence
Source identity	existing `ageintNNN` keys remain stable or new references are append-only
Verification	official, standards, public-domain, or scholarly URL is checked directly
Safety	method is converted into tabletop, audit, governance, or synthetic-data treatment
Reproducibility	another reviewer can rebuild the artifact from retained inputs
Rights review	privacy, IP, human-rights, workforce, and education impacts are considered where relevant

77.1.12 Cognitive Security and Inoculation Methods debrief protocol and reuse decision

Section anchor. Section 77.

Debrief by naming what the artifact can support, what it does not establish, what source changed, what risk was avoided by safe substitution, what human approval is still required, and when the appendix should be refreshed for CAMBREX Taxonomy of Manipulation Techniques (van der Linden); Python Prebunking Agent: Manipulation Detection + Inoculation Content Generation.

77.2 Cognitive degradation as a staged cascade

The Cloud Security Alliance Cognitive Degradation Resilience model treats an attack on an agent network not as a single breach but as a six-stage slide that stays below conventional alerting thresholds, illustrated for this appendix in Figure 154. Stage one is trigger injection, where adversarial inputs win a foothold in agent reasoning; stage two is resource starvation, in which context windows and compute are deliberately consumed to degrade decision quality; stage three is behavioral drift, where outputs deviate from policy without tripping alerts; stage four is memory entrenchment, where corrupted beliefs solidify in agent memory stores; stage five is functional override, where adversary objectives supersede the legitimate task; and stage six is systemic collapse, where coordinated agent behavior serves adversarial ends. The decisive observation is that the intervention window opens early – between resource starvation and behavioral drift – because once beliefs entrench in memory, remediation cost rises sharply [Alliance, 2025a].

Each stage is paired in the QSAF-BC control set with a named, testable countermeasure rather than a single catch-all monitor: starvation detection (BC-001) and token-overload limits (BC-002) defend the early stages, an entropy-drift monitor (BC-006) and a memory-integrity check (BC-007) defend the middle, and override resistance (BC-005) defends the late stages. Treat this cascade as a classroom tabletop: map a synthetic incident onto the six stages, identify which control would have fired first, and record the evidence a reviewer would need to confirm the agent recovered [Alliance, 2026]; [arXiv preprint authors, 2025a].

77.3 The decoherence-degradation isomorphism

The same dynamic appears one scale up. The CCDCOE reconception of cognitive warfare describes how an adversary degrades a human organization by attacking systemic invariants – shared trust, identity, and epistemic standards – driving it through initiation, uncertainty amplification, polarization, hardened competing frameworks, narrative capture, and a final state where the institution functions formally but can no longer coordinate. As Figure 155 makes explicit, those six human-organization phases map one-to-one onto the CDR degradation stages in an agent network, phase for phase from initiation to collapse [of Excellence, 2026]. The pedagogical payoff is that a single defensive vocabulary – early detection, drift monitoring, integrity of stored belief – transfers across both the human and the machine layer, which is why this appendix teaches them together rather than as separate disciplines.

77.3.1 Cognitive Security and Inoculation Methods visual navigation and evidence figures: purpose, source flow, and limits

The appendix uses Figure 154, Figure 155, and Figure 10 to map its evidence flow, safety boundaries, review artifacts, and refresh cues. Navigation links: Section 2, Section 76, Section 78.

77.3.2 Cognitive Security and Inoculation Methods runtime item map and source roster: generated rows and citation support

Safe curriculum treatment	Blocked source motif, audit-only	Allowed fixture	Rejected action	Required artifact	Citation spine
G.1 CAMBREX Taxonomy of Manipulation Techniques (van der Linden)	no blocked motif; source title used verbatim	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	-
Psychological inoculation and prebunking literacy review	G.2 retained for audit; operational wording transformed	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	[151, 2026]
G.3 NASA-TLX Cognitive Load Measurement Implementation	no blocked motif; source title used verbatim	sample messages, transparent labels, and opt-in classroom discussion cards	covert persuasion, microtargeting, impersonation, or campaign design	narrative-risk map and transparent education note	[179, 2026]
G.4 Active Inference Agent: FEP-Based Decision Under Uncertainty (pymdp)	no blocked motif; source title used verbatim	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	[106, 2026]
G.5 Bias Detection Pipeline: Automated ACH with Cognitive Bias Flagging	no blocked motif; source title used verbatim	sample messages, transparent labels, and opt-in classroom discussion cards	covert persuasion, microtargeting, impersonation, or campaign design	narrative-risk map and transparent education note	-

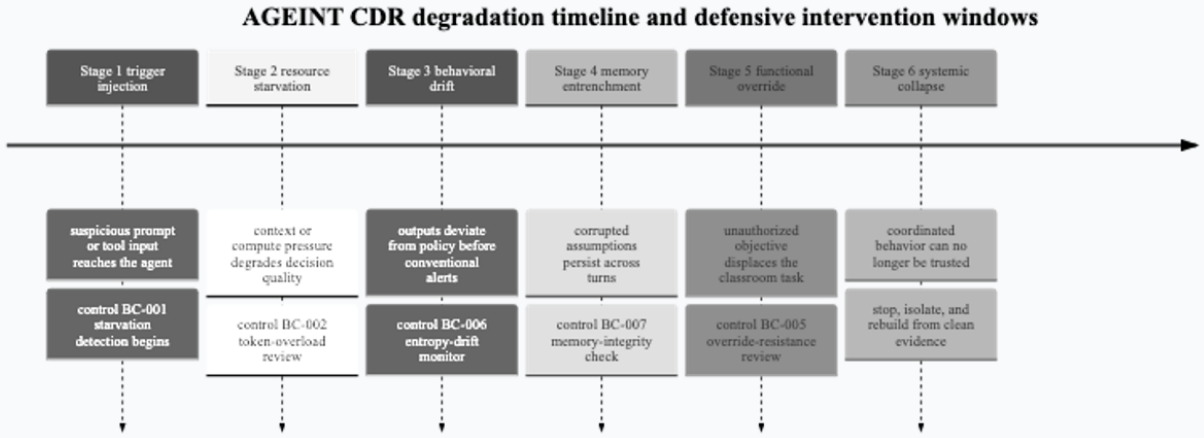


Figure 154: The CDR timeline places six degradation stages in chronological order and marks the control window where reviewer intervention can still preserve synthetic, evidence-bounded agent behavior. Its reader value is to make six chronological CDR stages, defensive QSAF-BC controls for starvation, overload, entropy drift, memory integrity, and override resistance, early-detection and decisive-intervention windows, and evidence-bounded classroom review boundary visible at a glance, with the cognitive security and inoculation methods appendix as the source section and defensive review as the boundary.

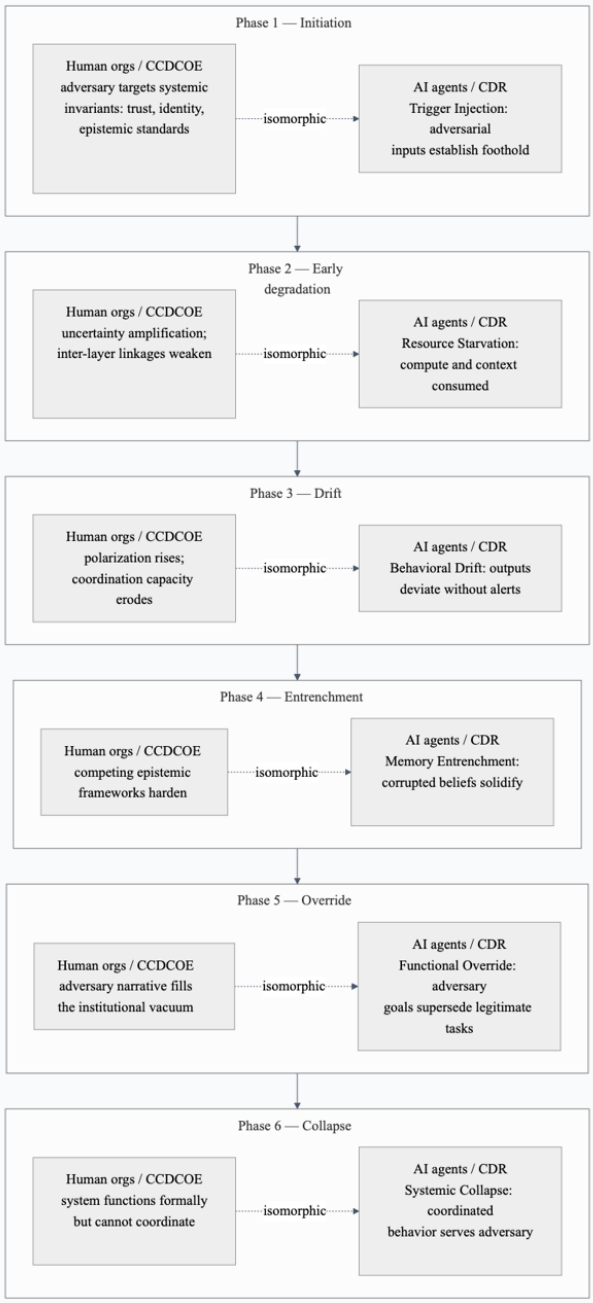


Figure 155: The six phases of CCDCOE cognitive decoherence in human organizations map one-to-one onto the CSA CDR cognitive-degradation stages in AI agent networks, exposing a shared adversarial dynamic. It is anchored to the cognitive security and inoculation methods appendix; use it to inspect Phase 1 — Initiation, Human orgs / CCDCOE adversary targets systemic invariants: trust, identity, epistemic standards, AI agents / CDR Trigger Injection: adversarial inputs establish foothold, and Phase 2 — Early degradation while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

78 Source Verification and Claim Ledger Workbook

The current appendix is an evidence workbook for reusable classroom methods. It is educational and evidence-bounded: examples remain synthetic, defensive, lawful, and bounded to owned labs, public sources, or tabletop exercises. Source-item focus: Source identity lock procedure for `ageint001` through `ageint231`, including title, URL, and citation-key stability checks; Append-only v2 reference workflow: discover with Perplexity if useful, verify direct official or standards URLs, then append new references after the locked range.

78.1 Source Verification and Claim Ledger Workbook workbook scope: purpose, safety envelope, and reuse decision

Section anchor. Section 78.

78.1.1 Source Verification and Claim Ledger Workbook operating purpose

Section anchor. Section 78.

The current appendix supports a reusable methods workbook. Each source item is treated as a reviewable classroom artifact rather than an operational instruction; examples begin with Source identity lock procedure for `ageint001` through `ageint231`, including title, URL, and citation-key stability checks; Append-only v2 reference workflow: discover with Perplexity if useful, verify direct official or standards URLs, then append new references after the locked range.

78.1.2 Source Verification and Claim Ledger Workbook allowed-input boundary

Section anchor. Section 78.

Allowed inputs for the current appendix are public official or scholarly sources, standards text, instructor-provided excerpts, synthetic datasets, owned-lab logs, toy examples, and generated rubrics that expose their provenance for Source identity lock procedure for `ageint001` through `ageint231`, including title, URL, and citation-key stability checks; Append-only v2 reference workflow: discover with Perplexity if useful, verify direct official or standards URLs, then append new references after the locked range.

78.1.3 Source Verification and Claim Ledger Workbook excluded-action boundary

Section anchor. Section 78.

Excluded actions for the current appendix are unauthorized collection, private-data processing, credential use, contact with real targets, live system interaction, exploit execution, deception, unsafe cyber-physical action, or external deployment while handling Source identity lock procedure for `ageint001` through `ageint231`, including title, URL, and citation-key stability checks; Append-only v2 reference workflow: discover with Perplexity if useful, verify direct official or standards URLs, then append new references after the locked range.

78.1.4 Source Verification and Claim Ledger Workbook expected artifact package

Section anchor. Section 78.

Expected appendix artifacts are a purpose statement, allowed-inputs card, excluded-actions card, source-lane map, provenance record, claim ledger, safe-substitution note, output schema, review rubric, and capstone handoff memo for Source identity lock procedure for `ageint001` through `ageint231`, including title, URL, and citation-key stability checks; Append-only v2 reference workflow: discover with Perplexity if useful, verify direct official or standards URLs, then append new references after the locked range.

78.1.5 Source Verification and Claim Ledger Workbook safe artifact schema

Section anchor. Section 78.

Field	Required evidence	Reject condition
Purpose	lawful educational, governance, research, or defensive purpose	vague operational objective or missing authority
Inputs	public, official, scholarly, synthetic, owned-lab, or instructor-provided material	private data, live target data, credentialed access, or unclear provenance
Transform	summary, comparison, rubric scoring, tabletop simulation, or audit review	collection expansion, external action, or unsafe system interaction
Output	memo, matrix, checklist, ledger, rubric, or debrief packet	deployable procedure, target package, or automated action plan
Reviewer	human reviewer, approval gate, revision note, and refresh owner	anonymous ownership or no escalation path

78.1.6 Source Verification and Claim Ledger Workbook input/output contract

Section anchor. Section 78.

Contract term	Input rule	Output rule
Source identity	retain `ageintNNN`, title, URL, and checked status	cite with Pandoc keys and avoid pasted raw URLs in prose
Accessibility	include plain-language labels, table headers, and figure alternatives	reject inaccessible figures, unlabeled tables, or single-modality evidence
Rights	identify affected groups, safeguards, and residual risk	preserve privacy, equality, access, contestability, and redress notes
Tooling	use allowlisted tools, visible prompts, logs, and stop conditions	keep outputs evidence-bounded, reversible, and human-reviewed
Refresh	record source, policy, standard, incident, or assessment trigger	assign an owner and date for revalidation

78.1.7 Source Verification and Claim Ledger Workbook failure cases and required responses

Section anchor. Section 78.

Failure case	Signal	Required response
Source laundering	claim cites an agent summary instead of a verified source	rebuild the claim ledger from direct sources
Boundary drift	exercise starts asking for live targets, private data, or external action	stop, substitute synthetic inputs, and document the block
Accessibility gap	learner cannot inspect, navigate, or complete the artifact	remediate and retest before reuse
Rights gap	affected group, safeguard, or redress path is missing	run HRIA/DPIA worksheet and escalate unresolved risk
Vendor opacity	tool owner, data use, logs, or exit path is unknown	replace tool or pause until procurement evidence exists

78.1.8 Source Verification and Claim Ledger Workbook evidence package schemas

Section anchor. Section 78.

Model and dataset card:

Field	Model card evidence	Dataset card evidence	Review gate
Intended use	accountable task, excluded uses, affected users, human reviewer, and accountable owner	Data Cards purpose statement, recommended use, prohibited reuse, stewardship owner, and affected stakeholder groups	claim is rejected if intended use, excluded use, affected users, or owner is missing
Provenance and collection	model family, version, supplier or lab, training cutoff, deployment context, and configuration hash	upstream source, collection process, annotation method, consent or authority basis, sensitivity class, and license	artifact is held if provenance, license, authority, or collection process is opaque
Composition and limits	capability boundary, known failure modes, tool permissions, context window limits, and unsupported conditions	population, sampling frame, coverage gaps, subgroup visibility, missingness, transformations, and known caveats	artifact is revised if population, coverage, or source limits are invisible
Evaluation and caveats	benchmark suite, task-specific tests, subgroup or context results, red-team findings, uncertainty notes, and failure examples	quality tests, label agreement, bias review, measurement limits, transformation log, and Data Cards answer-evaluation notes	empirical or performance claims are rejected unless test context, subgroup caveats, and uncertainty are visible
Lifecycle controls	release gate, rollback path, monitoring signal, incident threshold, refresh trigger, and model-card update owner	retention rule, access boundary, update cadence, deletion path, stewardship handoff, and dataset-card revision trigger	reuse is blocked without owner, retention, monitoring, rollback, and refresh evidence

Transparency notice:

Step	Artifact	Review gate
Public purpose	plain-language purpose, authority, affected service, and decision role	reader can tell why the system exists and where human judgment remains
Tool and data summary	model, data, supplier, provenance, validation, and accessibility summary	sensitive details are de-sensitized without hiding accountability fields
Impact and review	benefits, risks, safeguards, human review, appeal, and contact point	affected groups can identify recourse and oversight owners
Publication decision	publish, partially publish, delay, or hold decision with exemption rationale	non-public fields have a documented legal, security, privacy, or IP basis

Records retention and audit trail:

Record	Retained fields	Audit question
Source and prompt register	source identity, prompt version, tool allowlist, reviewer, timestamp, and caveat	Can a later reviewer reconstruct the evidentiary path without private or live data?
Decision and exception log	risk owner, accepted exception, compensating control, expiry date, and approval	Is every deviation time-bound, justified, and reviewable?
Artifact retention note	output type, sensitivity, access boundary, deletion rule, and refresh trigger	Does the retention choice match the educational purpose and rights impact?
Incident and remediation record	incident signal, containment action, root cause, owner, retest result, and closure date	Can the same failure be detected and prevented in the next reuse cycle?

Release and change-control gate:

Gate	Release evidence	Block condition
Scope freeze	accountable use case, excluded actions, tool profile, and data boundary	scope expands to external action, live data, or an unreviewed capability
Security and rights review	privacy, accessibility, security, bias, and human-review checks	rights impact, vulnerability, or accessibility issue has no owner
Version and rollback	model or prompt version, changelog, test fixture, and rollback path	change cannot be reproduced, compared, or reverted
Post-release monitoring	monitoring signal, incident threshold, refresh trigger, and owner	deployment or reuse occurs without logging and retest commitments

Risk exception memo:

Field	Minimum content	Approval rule
Exception requested	what requirement cannot be met, why, affected groups, and duration	exception must be specific, time-bound, and tied to a compensating control
Risk basis	likelihood, impact, evidence, uncertainty, alternatives, and rejected options	unsupported confidence or missing alternatives returns the memo for revision
Compensating control	human review, monitoring, access limit, disclosure, remediation, and owner	control must reduce risk without creating an operational workaround

Field	Minimum content	Approval rule
Expiry and retest	expiry date, retest condition, review cadence, and closure criteria	open-ended exceptions are rejected

Learner support and accommodation plan:

Need	Support	Evidence
Access and modality	captions, alt text, keyboard path, plain-language summary, and structured tables	accessibility checklist, defect log, and retest result
Cognitive load	worked examples, staged release, glossary, checklist, and optional practice fixture	UDL design note and learner feedback record
Assessment fairness	allowed-tool statement, AI-use declaration, alternative submission mode, and transparent rubric	assessment-integrity note and accommodation record
Feedback and remediation	revision path, office-hour prompt, example correction, and due-date flexibility policy	feedback log and instructor disposition

Instructor question bank:

Question type	Prompt	Evidence
Source challenge	Which claim would fail if the strongest source were removed or downgraded?	claim ledger revision and source-lane note
Boundary challenge	Where could this exercise drift from analysis into action, and what safe substitute prevents it?	safe-substitution decision and excluded-action card
Rights challenge	Which affected group, accessibility need, privacy interest, or redress path is under-specified?	HRIA/DPIA update and accommodation note
Assurance challenge	What failure would the current evaluation miss, and what retest would reveal it?	adversarial assurance retest and remediation owner

Remediation backlog:

Backlog item	Trigger	Closure evidence
Unverified claim	claim lacks a guide citation or directly verified anchor	verified source, removed claim, or explicit source-guide context note
Unsafe phrasing	wording implies live targeting, external action, exploitation, manipulation, or unsafe control	safe substitute, blocked context, and reviewer sign-off
Accessibility defect	artifact cannot be inspected through an expected assistive or alternative workflow	defect fix, alternative means, and retest result
Assurance gap	evaluation, release, exception, incident, or vendor evidence is incomplete	owner, due date, retest, and accepted disposition

78.1.9 Source Verification and Claim Ledger Workbook rubric scoring bands

Section anchor. Section 78.

Band	Evidence standard	Disposition
4 - ready	source identity, accessibility, rights, safety, and reviewer evidence are complete	may be reused after normal refresh review
3 - revise	one evidence field is incomplete but risk is bounded and remediable	revise before reuse
2 - hold	multiple evidence fields are incomplete or ownership is unclear	hold for instructor and assurance review
1 - reject	unsafe action, private data, inaccessible artifact, or unverified claim appears	reject and rebuild from safe inputs

78.1.10 Source Verification and Claim Ledger Workbook refresh evidence

Section anchor. Section 78.

Evidence item	Refresh trigger	Retained support
Source lane	official source, standard, or legal text changes	checked-as-of date and source note
Safety treatment	operational wording or unsafe motif appears	safe-substitution decision and blocked context
Accessibility	WCAG, UDL, or institutional accessibility duty changes	defect log, retest result, and owner
Rights	privacy, human-rights, public transparency, or education guidance changes	HRIA/DPIA revision note
Vendor/tool	contract, data-use, incident, or model capability changes	procurement packet and incident review

78.1.11 Source Verification and Claim Ledger Workbook validation rubric

Section anchor. Section 78.

Criterion	Passing evidence
Source identity	existing `ageintNNN` keys remain stable or new references are append-only
Verification	official, standards, public-domain, or scholarly URL is checked directly
Safety	method is converted into tabletop, audit, governance, or synthetic-data treatment
Reproducibility	another reviewer can rebuild the artifact from retained inputs
Rights review	privacy, IP, human-rights, workforce, and education impacts are considered where relevant

78.1.12 Source Verification and Claim Ledger Workbook debrief protocol and reuse decision

Section anchor. Section 78.

Debrief by naming what the artifact can support, what it does not establish, what source changed, what risk was avoided by safe substitution, what human approval is still required, and when the appendix should be refreshed for Source identity lock procedure for `ageint001` through `ageint231`, including title, URL, and citation-key stability checks; Append-only v2 reference workflow: discover with Perplexity if useful, verify direct official or standards URLs, then append new references after the locked range.

78.2 Source verification workflow

Section anchor. Section 78.

The source-verification and claim-ledger workbook preserves `ageint001` through `ageint231`, appends new references after the locked range, and records lane, tier, checked date, verification method, claim scope, refresh cadence, and refresh trigger for every curated anchor.

Source lane	Anchor count	Refresh cadence	Claim scope
accessibility_digital_inclusion	4	annual, quarterly, semiannual	4 scoped claim families
active_measures_attribution	1	annual	Supports bounded AGEINT discussion of active_measures_attribution and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
active_measures_disinformation	1	annual	Supports bounded AGEINT discussion of active_measures_disinformation and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
active_measures_information_operations	1	annual	Supports bounded AGEINT discussion of active_measures_information_operations and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
adversarial_ai_security	1	semiannual	Supports bounded AGEINT discussion of adversarial_ai_security and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
agent_foundations	2	semiannual	Supports bounded AGEINT discussion of agent_foundations and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
agent_incident_response	7	annual, quarterly, semiannual	7 scoped claim families
agent_interoperability_standards	12	annual, quarterly, semiannual	12 scoped claim families
agentic_ai_governance	21	annual	8 scoped claim families
agentic_ai_security	2	annual, semiannual	2 scoped claim families
agentic_ai_security_governance	1	quarterly	agentic AI adoption and security-governance context, not an AGEINT benchmark
agentic_analytic_assistance	1	annual	Supports bounded claims that AI-enabled reasoning systems can assist evidence discovery and reasoning review while retaining analyst responsibility.

Source lane	Anchor count	Refresh cadence	Claim scope
agentic_design_principles	1	semiannual	Supports bounded AGEINT discussion of agentic_design_principles and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
agentic_framework_docs	3	semiannual	Supports bounded AGEINT discussion of agentic_framework_docs and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
agentic_memory	1	semiannual	Supports bounded AGEINT discussion of agentic_memory and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
agentic_reasoning	1	semiannual	Supports bounded AGEINT discussion of agentic_reasoning and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
ai_conformity_compliance	7	annual, quarterly, semiannual	7 scoped claim families
ai_enabled_analysis_boundary	9	annual, semiannual	9 scoped claim families
ai_ethics_data_governance	10	annual	curriculum grounding and source-backed synthesis
ai_red_team_assurance	14	annual, quarterly, semiannual	14 scoped claim families
algorithmic_transparency_reporting	2	quarterly	2 scoped claim families
analytic_cognition_and_bias	6	annual	6 scoped claim families
analytic_epistemology	1	annual	epistemic-framing support for calibrated claims and reviewer challengeability
analytic_method_design	3	annual	3 scoped claim families
analytic_method_pedagogy	9	annual	9 scoped claim families
analytic_outreach_governance	1	annual	analytic-outreach governance support for expert engagement and risk controls
analytic_product_dissemination	1	annual	analytic-product utility, discoverability, and dissemination-governance support
analytic_production_workflow	1	annual	workflow and analytic-production support for iterative, reviewable tradecraft artifacts
analytic_tradecraft	7	annual	2 scoped claim families
analytic_tradecraft_evidence	5	annual	5 scoped claim families
analytic_tradecraft_forecasting	2	annual	Supports bounded AGEINT discussion of analytic_tradecraft_forecasting and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
analytic_uncertainty_language	4	annual	4 scoped claim families

Source lane	Anchor count	Refresh cadence	Claim scope
apt_threat_intelligence	3	semiannual	Supports bounded AGEINT discussion of apt_threat_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
assurance_evaluation_evidence	8	annual, quarterly, semiannual	8 scoped claim families
classification_marking_governance	1	annual	classification-marking context for caveat and dissemination-boundary lessons
cognitive_active_inference	9	annual	9 scoped claim families
cognitive_bias_foundations	2	annual	Supports bounded AGEINT discussion of cognitive_bias_foundations and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
cognitive_influence_security	13	annual	10 scoped claim families
cognitive_performance	4	annual	Supports bounded AGEINT discussion of cognitive_performance and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
cognitive_resilience_evidence	1	annual	Peer-reviewed Science Advances study testing psychological inoculation videos for improving misinformation resilience at scale, with bounded transfer from measured outcomes to curriculum claims
cognitive_security_inoculation	2	annual	Supports bounded AGEINT discussion of cognitive_security_inoculation and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
cognitive_security_misinformation	1	annual	Supports bounded AGEINT discussion of cognitive_security_misinformation and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
collection_management	2	annual	curriculum grounding and source-backed synthesis
collection_management_doctrine	1	annual	Supports bounded AGEINT discussion of collection_management_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
counterintelligence_program_governance	2	annual, quarterly	2 scoped claim families
counterintelligence_source_integrity	7	annual	6 scoped claim families

Source lane	Anchor count	Refresh cadence	Claim scope
counterintelligence_strategy	2	annual	Supports bounded AGEINT discussion of counterintelligence_strategy and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
cross_border_data_spaces	4	semiannual	4 scoped claim families
cryptographic_standards	1	semiannual	Supports bounded AGEINT discussion of cryptographic_standards and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
cryptography_standards	3	semiannual	Supports bounded AGEINT discussion of cryptography_standards and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
current_threat_baseline	1	annual	public threat-context grounding and warning-topic baseline, not operational targeting or AGEINT benchmark evidence
cyber_defense_guidance_index	1	quarterly	defensive cyber guidance index support for source routing and refresh duties
cyber_threat_intelligence	17	annual, semiannual	8 scoped claim families
dataset_documentation	2	annual	2 scoped claim families
declassified_analytic_history	2	annual	2 scoped claim families
declassified_reconnaissance_history	1	annual	declassified reconnaissance history support for historical and GEOINT source-provenance lessons
defense_osint_governance	1	annual	public OSINT governance and professionalization support, not collection procedure or live targeting guidance
disinformation_cognitive_psychology	1	annual	Supports bounded AGEINT discussion of disinformation_cognitive_psychology and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
disinformation_misinformation_science	1	annual	Supports bounded AGEINT discussion of disinformation_misinformation_science and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
economic_security_review	1	annual	economic-security and due-diligence governance support for threat-analysis framing
education_assessment	6	annual, semiannual	6 scoped claim families

Source lane	Anchor count	Refresh cadence	Claim scope
ethics_of_intelligence	3	annual	Supports bounded AGEINT discussion of ethics_of_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
financial_economic_security	8	annual	curriculum grounding and source-backed synthesis
finint_aml_cft_international	2	annual	Supports bounded AGEINT discussion of finint_aml_cft_international and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
finint_international_cooperation	1	annual	Supports bounded AGEINT discussion of finint_international_cooperation and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
finint_sar_reporting	1	annual	Supports bounded AGEINT discussion of finint_sar_reporting and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
forecasting_calibration_evidence	6	annual	6 scoped claim families
foreign_disclosure_governance	1	annual	foreign-disclosure governance support for release-boundary and control-marking lessons
geoint_data_governance	1	annual	GEOINT data-governance and digital-transformation context for modular source substrate claims
geoint_doctrine	2	annual	Supports bounded AGEINT discussion of geoint_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
geoint_professional_doctrine	1	annual	GEOINT doctrine and geospatial-intelligence framing support
geoint_tradecraft	1	annual	Supports bounded AGEINT discussion of geoint_tradecraft and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
governed_intelligence_cycle	2	annual	curriculum grounding and source-backed synthesis

Source lane	Anchor count	Refresh cadence	Claim scope
gray_zone_competition_doctrine	1	annual	Supports bounded AGEINT discussion of gray_zone_competition_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
historical_declassified_sources	4	annual	curriculum grounding and source-backed synthesis
historical_ics_incidents	4	semiannual	Supports bounded AGEINT discussion of historical_ics_incidents and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
human_rights_governance	6	annual, semiannual	6 scoped claim families
humint_doctrine	4	annual	Supports bounded AGEINT discussion of humint_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
humint_oversight_history	1	annual	Supports bounded AGEINT discussion of humint_oversight_history and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
hybrid_warfare_doctrine	1	annual	Supports bounded AGEINT discussion of hybrid_warfare_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
hybrid_warfare_stratcom	1	annual	Supports bounded AGEINT discussion of hybrid_warfare_stratcom and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
ic_information_environment_risk	2	annual	2 scoped claim families
ic_public_transparency	7	quarterly	7 scoped claim families
ics_ot_defense	10	annual	curriculum grounding and source-backed synthesis
ics_ot_security_standards	3	semiannual	Supports bounded AGEINT discussion of ics_ot_security_standards and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.

Source lane	Anchor count	Refresh cadence	Claim scope
imint_joint_intelligence_doctrine	1	annual	Supports bounded AGEINT discussion of imint_joint_intelligence_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
information_operations_doctrine	1	annual	Supports bounded AGEINT discussion of information_operations_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
integrated_mission_management	1	annual	mission-management governance support for requirements-to-evidence substrate design
intelligence_diplomacy_governance	1	annual	governance context for intelligence diplomacy and partner-engagement boundaries
intelligence_failure_postmortem	9	annual, biennial	9 scoped claim families
intelligence_history_american	1	annual	Supports bounded AGEINT discussion of intelligence_history_american and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
intelligence_history_british_allied	1	annual	Supports bounded AGEINT discussion of intelligence_history_british_allied and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
intelligence_history_soviet	2	annual	Supports bounded AGEINT discussion of intelligence_history_soviet and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
intelligence_profession_literature	4	annual	4 scoped claim families
intelligence_writing_and_review	3	annual	3 scoped claim families
irregular_warfare_strategy	1	annual	Supports bounded AGEINT discussion of irregular_warfare_strategy and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
learner_support_accommodations	1	semiannual	learner support plans, accessibility exception documentation, alternative means, and artifact remediation

Source lane	Anchor count	Refresh cadence	Claim scope
legal_authorities_intelligence_collection	1	annual	Supports bounded AGEINT discussion of legal_authorities_intelligence_collection and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
legal_authorities_surveillance	3	annual	Supports bounded AGEINT discussion of legal_authorities_surveillance and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
legal_oversight	9	annual	curriculum grounding and source-backed synthesis
legal_oversight_intelligence	1	annual	Supports bounded AGEINT discussion of legal_oversight_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
llm_architecture	1	semiannual	Supports bounded AGEINT discussion of llm_architecture and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
llm_evaluation	2	semiannual	Supports bounded AGEINT discussion of llm_evaluation and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
model_card_reporting	1	annual	model documentation cards, intended-use statements, evaluation caveats, and release notes
model_data_provenance	14	annual, quarterly, semiannual	14 scoped claim families
multi_agent_frameworks	1	semiannual	Supports bounded AGEINT discussion of multi_agent_frameworks and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
national_intelligence_governance	1	annual	IC governance and national-intelligence production context
non_state_engagement_governance	1	annual	non-state engagement governance support for source, outreach, and no-tasking boundaries
opsec_doctrine_governance	1	biennial	Provides official historical OPSEC policy context for critical-information protection and public doctrine framing; not an operational OPSEC playbook.

Source lane	Anchor count	Refresh cadence	Claim scope
osint_doctrine	3	annual	Supports bounded AGEINT discussion of osint_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
osint_geoint	6	annual	2 scoped claim families
osint_methodology	1	annual	Supports bounded AGEINT discussion of osint_methodology and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
privacy_ip_governance	3	annual	curriculum grounding and source-backed synthesis
procurement_performance_monitoring	1	quarterly	AI procurement monitoring, vendor demonstrations, acquisition criteria, QASP evidence, and performance review
procurement_vendor_governance	4	annual, quarterly, semiannual	4 scoped claim families
psyop_miso_doctrine	1	annual	Supports bounded AGEINT discussion of psyop_miso_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
public_sector_agentic_ai	5	quarterly, semiannual	5 scoped claim families
public_sector_transparency	3	annual, quarterly, semiannual	3 scoped claim families
records_retention_auditability	5	annual, quarterly, semiannual	5 scoped claim families
rights_impact_privacy	4	annual, quarterly, semiannual	4 scoped claim families
risk_exception_governance	1	quarterly	risk exception governance, AI maturity plans, data traceability, public trust, and oversight capacity
sat_evaluation_evidence	13	annual	13 scoped claim families
secure_release_change_control	9	annual, quarterly, semiannual	9 scoped claim families
sigint_emanations_intelligence	1	annual	Supports bounded AGEINT discussion of sigint_emanations_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
sigint_history	1	annual	Supports bounded AGEINT discussion of sigint_history and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
sigint_oversight_history	1	annual	Supports bounded AGEINT discussion of sigint_oversight_history and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.

Source lane	Anchor count	Refresh cadence	Claim scope
social_engineering_influence_psychology	1	annual	Supports bounded AGEINT discussion of social_engineering_influence_psychology and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
source_construction_reporting	1	annual	PRISMA-S reporting guideline for documenting literature searches, search strategies, information sources, limits, records, and reproducibility details
special_operations_doctrine	1	annual	Supports bounded AGEINT discussion of special_operations_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
supply_chain_intelligence_attacks	3	semiannual	Supports bounded AGEINT discussion of supply_chain_intelligence_attacks and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
supply_chain_risk_governance	1	annual	supply-chain risk governance support for defensive procurement and assurance lessons
synthetic_media_provenance	4	annual, semiannual	4 scoped claim families
tearlines_and_release_governance	1	annual	tearline and release-governance support for public-facing evidence boundaries
threat_intel_sharing_standards	1	semiannual	Supports bounded AGEINT discussion of threat_intel_sharing_standards and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
tool_use_agents	2	semiannual	Supports bounded AGEINT discussion of tool_use_agents and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.
warning_intelligence	3	annual	3 scoped claim families
workforce_governance	5	annual, quarterly, semiannual	5 scoped claim families

78.3 Source refresh evidence

Section anchor. Section 78.

Object	Lineage field	Quality gate
Source citation	`ageintNNN`, title, URL, checked date, and source identity status	citation key resolves and reference identity is locked or append-only
Verified anchor	lane, tier, verification method, claim scope, stakeholder role, and assurance use	direct official, standards, public-domain, or scholarly URL was reviewed
Dataset or scenario	origin, license, sensitivity class, transformations, and retention rule	public, synthetic, owned-lab, or instructor-provided data only
Agent transcript	prompt, model context, tool allowlist, budget, reviewer, and blocked actions	no external action, live target, private data, or unsafe cyber-physical step

Final artifact	claim ledger, uncertainty note, accessibility status, rights review, and refresh owner	another reviewer can reproduce and challenge the artifact

78.4 HRIA/DPIA evidence bridge

Section anchor. Section 78.

Dimension	Prompt	Evidence
Purpose and authority	What public, educational, or defensive purpose justifies the processing or analysis?	scope card, excluded-action list, and decision owner
Data subjects and affected groups	Who could be affected directly, indirectly, or through downstream reuse?	stakeholder map, vulnerability note, and accessibility considerations
High-risk processing trigger	Does the activity involve sensitive data, profiling, automated evaluation, large-scale processing, or systematic monitoring?	DPIA trigger checklist and mitigation owner
Rights and safeguards	How are privacy, equality, expression, access, contestability, and redress protected?	rights-impact note, safeguard register, and escalation path
Residual risk and refresh	What remains uncertain, who accepts it, and what source or incident would reopen review?	residual-risk decision, review date, and source-refresh trigger

78.4.1 Source Verification and Claim Ledger Workbook visual navigation and evidence figures: purpose, source flow, and limits

The appendix uses Figure 156, Figure 157, Figure 158, Figure 159, Figure 160, Figure 161, Figure 162, and Figure 10 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.

Navigation links: Section 2, Section 77, Section 79.

78.4.2 Source Verification and Claim Ledger Workbook runtime item map and source roster: generated rows and citation support

Safe curriculum treatment	Blocked source motif, audit-only	Allowed fixture	Rejected action	Required artifact	Citation spine
H.1 Source identity lock procedure for `ageint001` through `ageint231`, including title, URL, and citation-key stability checks	no blocked motif; source title used verbatim	sample role records, ethics cards, and reviewer notes	impersonation, contact activity, elicitation, handling, or source exposure	source-protection ethics memo and escalation path	[235, 2026]; [237, 2026]
H.2 Append-only v2 reference workflow: discover with Perplexity if useful, verify direct official or standards URLs, then append new references after the locked range	no blocked motif; source title used verbatim	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	[232, 2026]; [234, 2026]
H.3 Source-lane metadata worksheet: lane, tier, checked-as-of date, verification method, claim scope, refresh cadence, and refresh trigger	no blocked motif; source title used verbatim	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	[238, 2026]; [266, 2026]
H.4 Claim/evidence ledger template for separating observation, inference, confidence, uncertainty, rights impact, and reviewer decision	no blocked motif; source title used verbatim	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	[237, 2026]; [269, 2026]
H.5 Safe refresh protocol for broken URLs, superseded standards, legal updates, source drift, and instructor debrief findings	no blocked motif; source title used verbatim	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	[251, 2026]; [252, 2026]; [270, 2026]

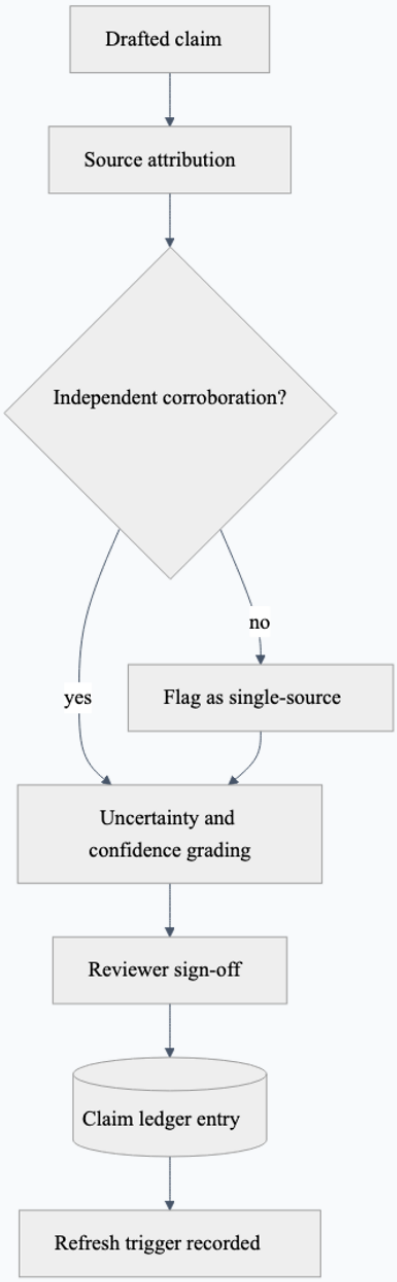


Figure 156: The claim-ledger workbook routes each claim through source attribution, corroboration, and uncertainty grading, recording a reviewer and a refresh trigger before the claim is accepted. It is anchored to the source verification and claim ledger workbook appendix; use it to inspect Drafted claim, Source attribution, Flag as single-source, and Uncertainty and confidence grading while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

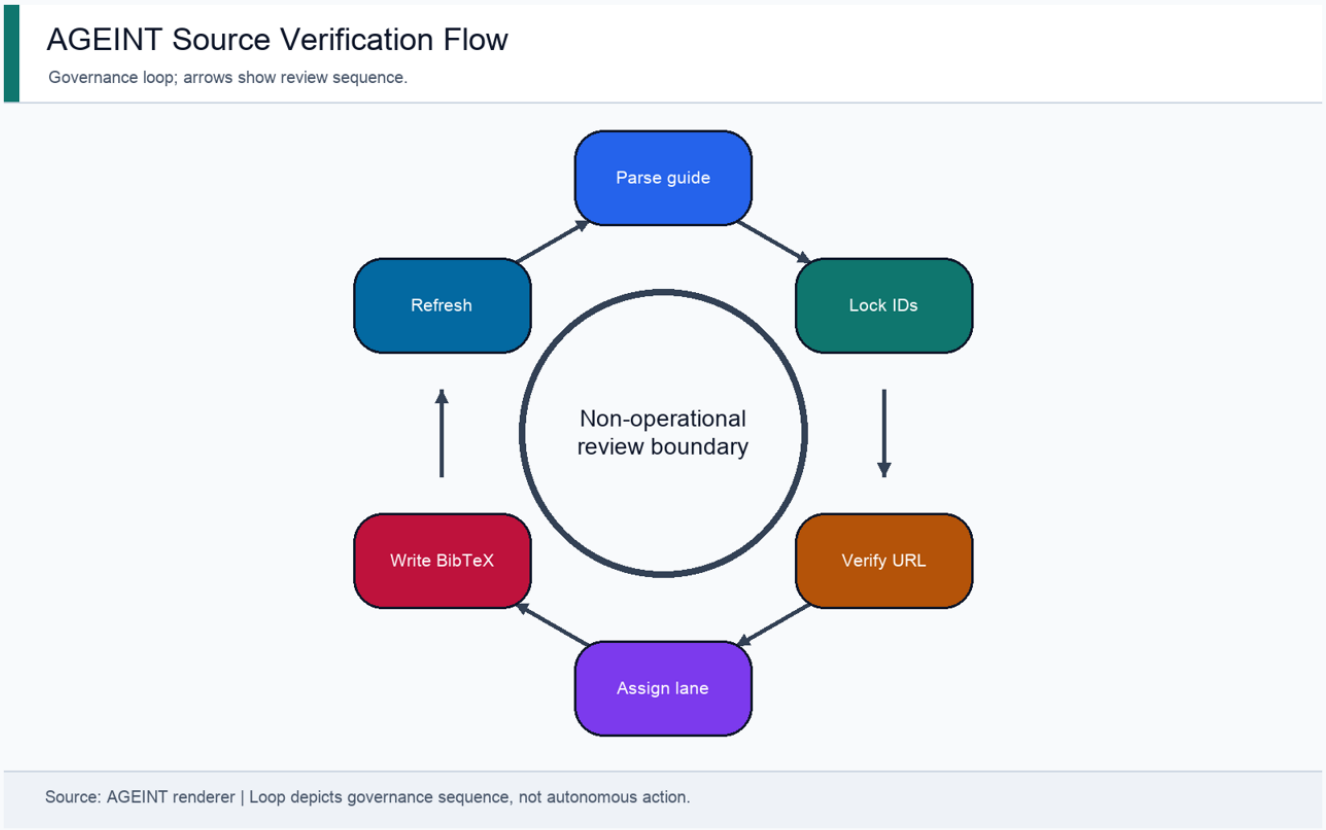


Figure 157: The source-verification workflow connects locked references, v2 source lanes, checked dates, and refresh triggers. The captioned view belongs to the source verification and claim ledger workbook appendix and should be read as a map of source verification flow steps, decision gates, owner handoffs, refresh triggers, and closure evidence, not as a capability score or live-task instruction.

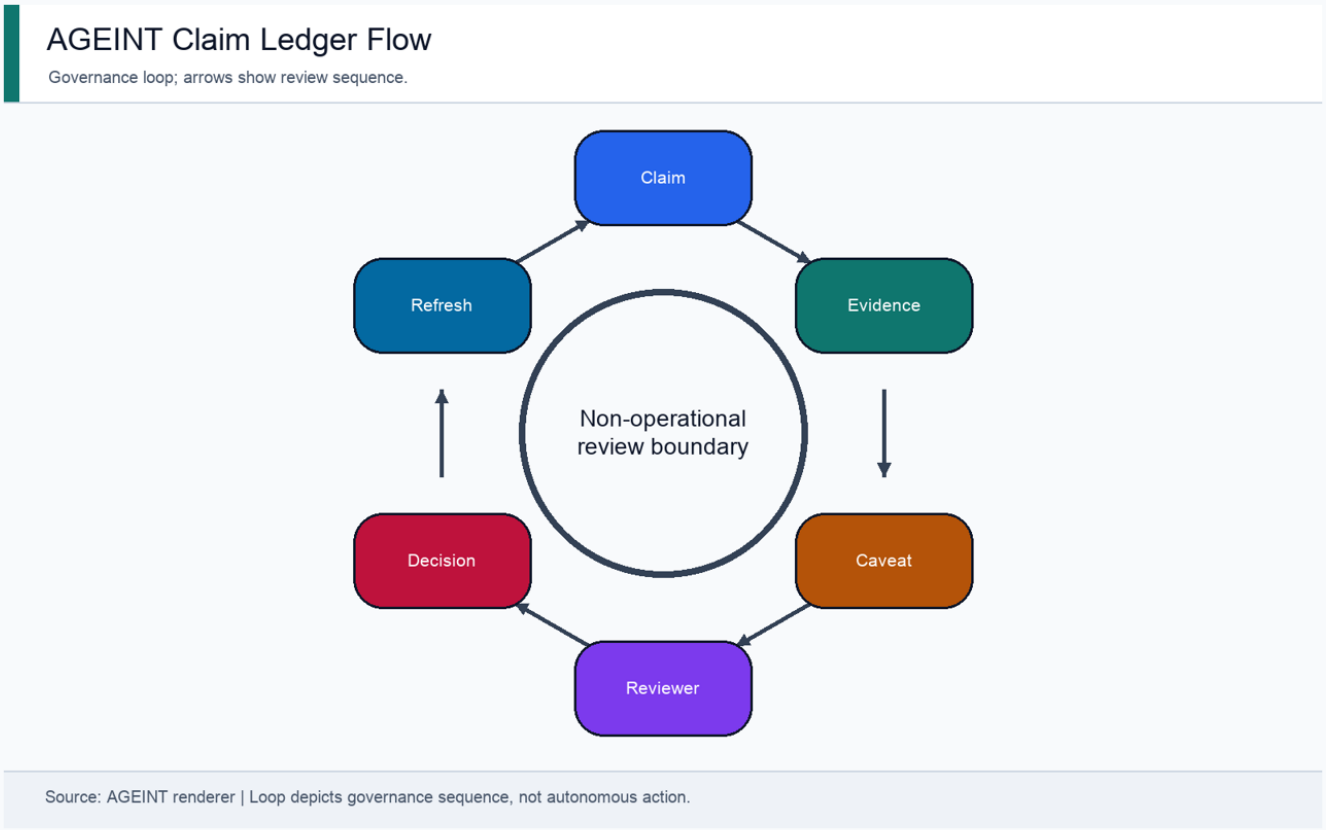


Figure 158: The claim-ledger flow keeps evidence, uncertainty, review ownership, and refresh triggers visible. It is anchored to the source verification and claim ledger workbook appendix; use it to inspect claim ledger flow steps, decision gates, owner handoffs, refresh triggers, and closure evidence while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

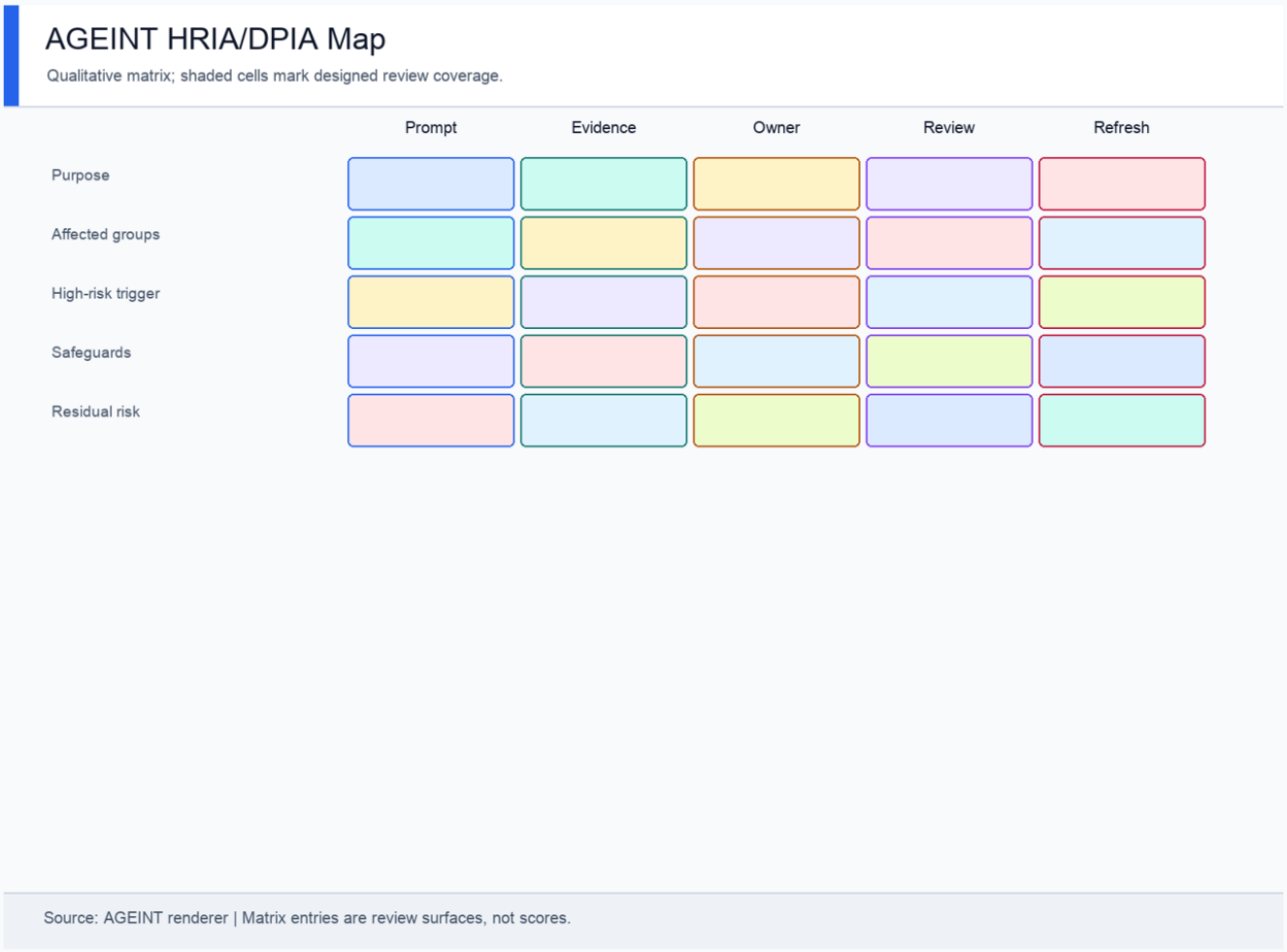


Figure 159: The HRIA/DPIA map separates purpose, affected groups, high-risk triggers, safeguards, and residual risk. The captioned view belongs to the source verification and claim ledger workbook appendix and should be read as a map of hria dpia map fields, row and column obligations, source records, reviewer decisions, and closure evidence, not as a capability score or live-task instruction.

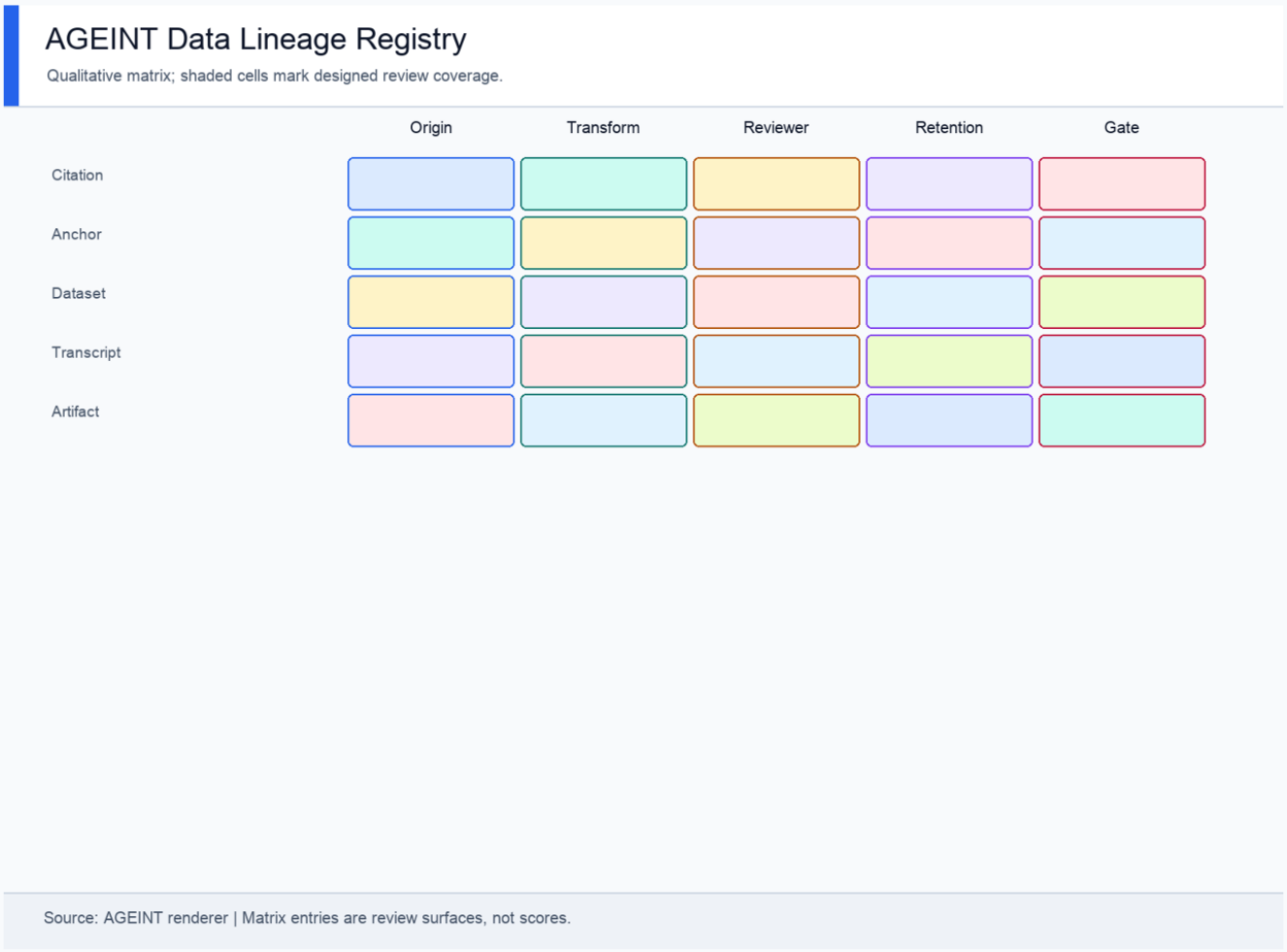


Figure 160: The data lineage registry traces source citations, verified anchors, datasets, transcripts, and final artifacts. The captioned view belongs to the source verification and claim ledger workbook appendix and should be read as a map of data lineage registry fields, row and column obligations, source records, reviewer decisions, and closure evidence, not as a capability score or live-task instruction.

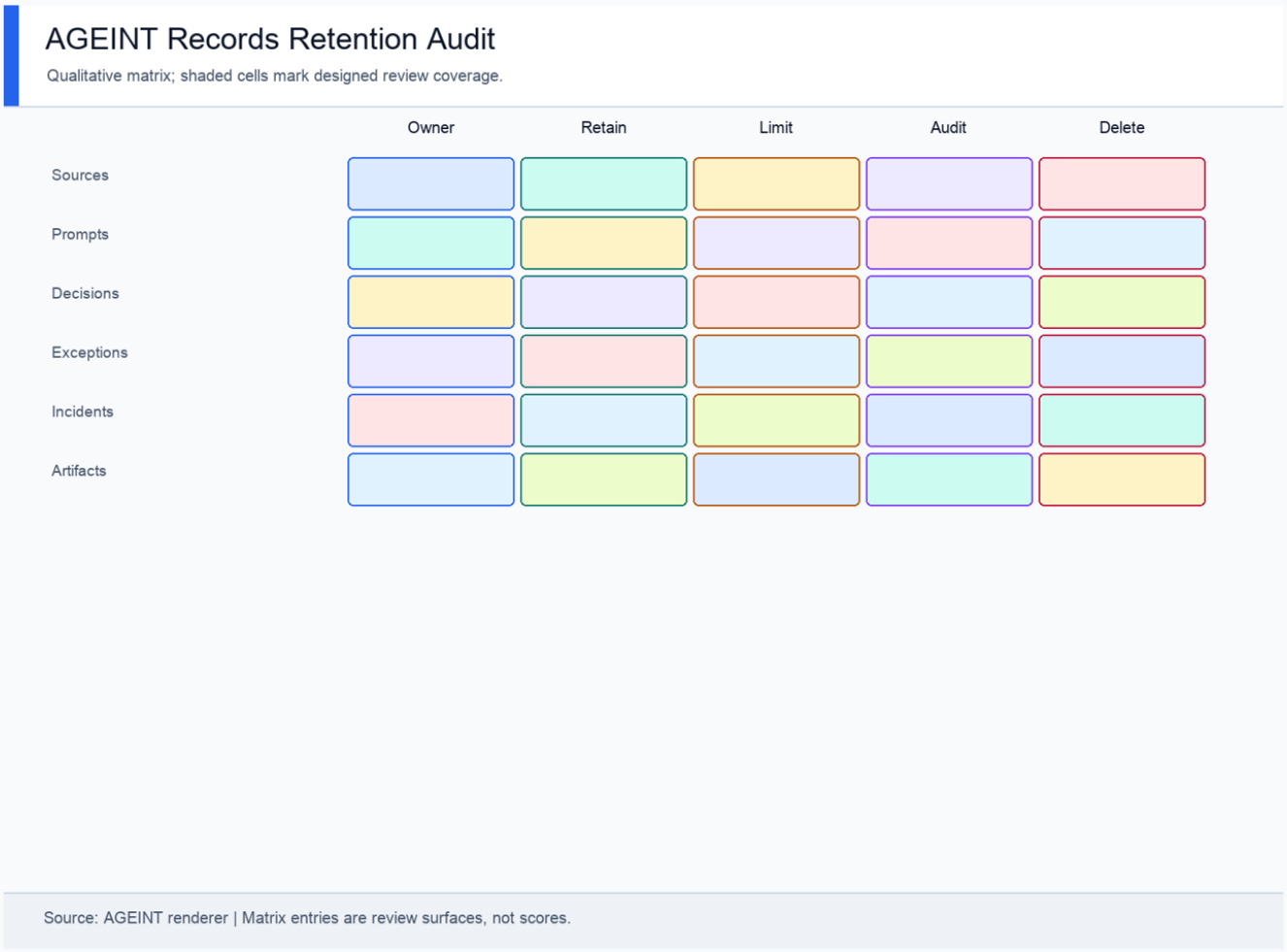


Figure 161: The records retention audit ties retained records to audit questions, exceptions, and remediation evidence. It is anchored to the source verification and claim ledger workbook appendix; use it to inspect records retention audit fields, row and column obligations, source records, reviewer decisions, and closure evidence while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

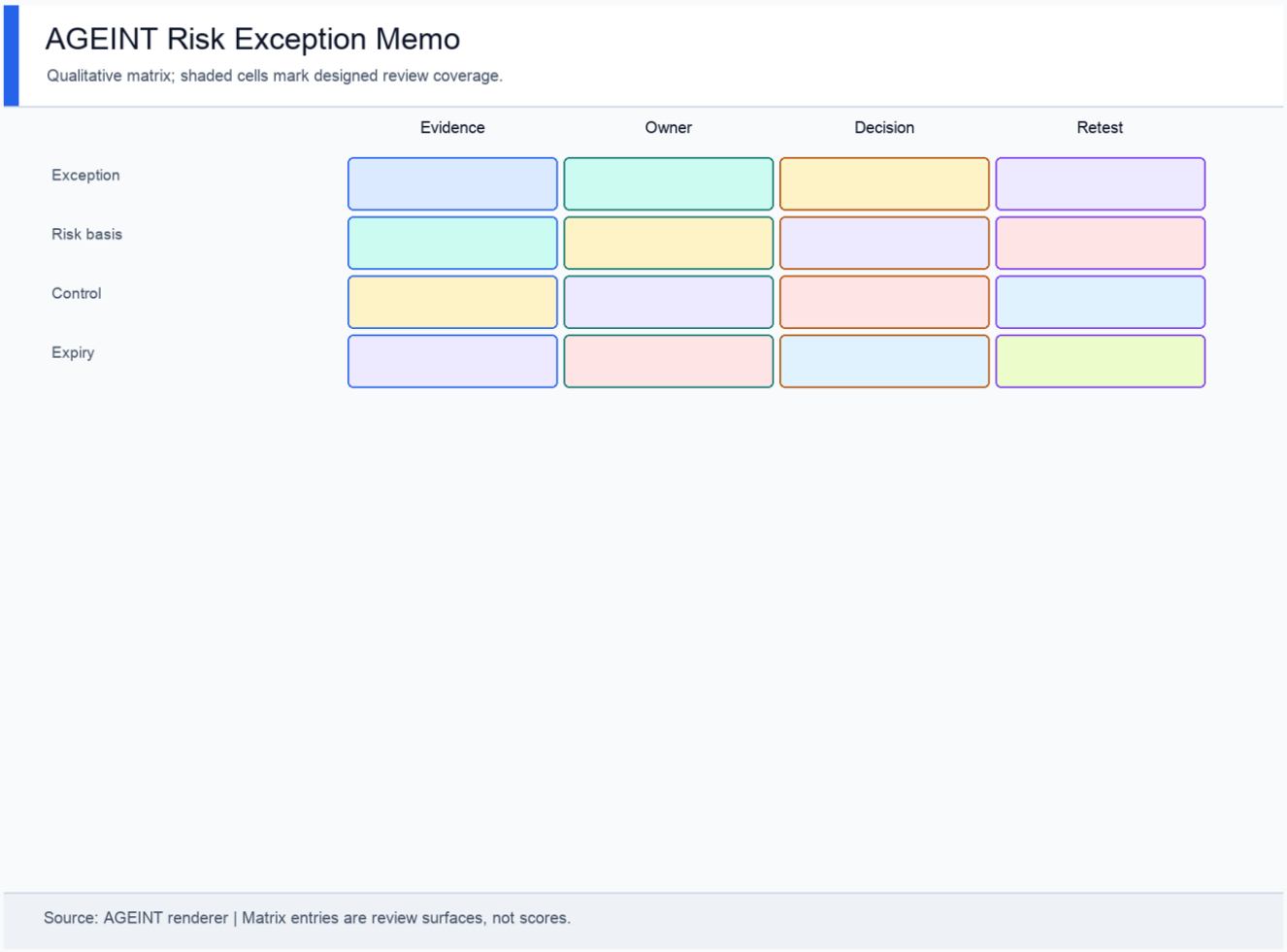


Figure 162: The risk exception memo keeps exception basis, compensating controls, expiry, and retest evidence together. In the source verification and claim ledger workbook appendix, it lets readers compare risk exception memo fields, row and column obligations, source records, reviewer decisions, and closure evidence so the visual functions as a traceable course aid rather than an unscoped assertion.

79 Instructor Capstone, Rubric, and Red-Team Review Pack

The current appendix is an evidence workbook for reusable classroom methods. It is educational and evidence-bounded: examples remain synthetic, defensive, lawful, and bounded to owned labs, public sources, or tabletop exercises. Source-item focus: Capstone authorization card: learning question, allowed inputs, excluded actions, human oversight, and stop conditions; Instructor rubric for source quality, analytic rigor, agent control, rights mapping, reproducibility, and safe substitution.

79.1 Instructor Capstone, Rubric, and Red-Team Review Pack workbook scope: purpose, safety envelope, and reuse decision

Section anchor. Section 79.

79.1.1 Instructor Capstone, Rubric, and Red-Team Review Pack operating purpose

Section anchor. Section 79.

The current appendix supports a reusable methods workbook. Each source item is treated as a reviewable classroom artifact rather than an operational instruction; examples begin with Capstone authorization card: learning question, allowed inputs, excluded actions, human oversight, and stop conditions; Instructor rubric for source quality, analytic rigor, agent control, rights mapping, reproducibility, and safe substitution.

79.1.2 Instructor Capstone, Rubric, and Red-Team Review Pack allowed-input boundary

Section anchor. Section 79.

Allowed inputs for the current appendix are public official or scholarly sources, standards text, instructor-provided excerpts, synthetic datasets, owned-lab logs, toy examples, and generated rubrics that expose their provenance for Capstone authorization card: learning question, allowed inputs, excluded actions, human oversight, and stop conditions; Instructor rubric for source quality, analytic rigor, agent control, rights mapping, reproducibility, and safe substitution.

79.1.3 Instructor Capstone, Rubric, and Red-Team Review Pack excluded-action boundary

Section anchor. Section 79.

Excluded actions for the current appendix are unauthorized collection, private-data processing, credential use, contact with real targets, live system interaction, exploit execution, deception, unsafe cyber-physical action, or external deployment while handling Capstone authorization card: learning question, allowed inputs, excluded actions, human oversight, and stop conditions; Instructor rubric for source quality, analytic rigor, agent control, rights mapping, reproducibility, and safe substitution.

79.1.4 Instructor Capstone, Rubric, and Red-Team Review Pack expected artifact package

Section anchor. Section 79.

Expected appendix artifacts are a purpose statement, allowed-inputs card, excluded-actions card, source-lane map, provenance record, claim ledger, safe-substitution note, output schema, review rubric, and capstone handoff memo for Capstone authorization card: learning question, allowed inputs, excluded actions, human oversight, and stop conditions; Instructor rubric for source quality, analytic rigor, agent control, rights mapping, reproducibility, and safe substitution.

79.1.5 Instructor Capstone, Rubric, and Red-Team Review Pack safe artifact schema

Section anchor. Section 79.

Field	Required evidence	Reject condition
Purpose	lawful educational, governance, research, or defensive purpose	vague operational objective or missing authority
Inputs	public, official, scholarly, synthetic, owned-lab, or instructor-provided material	private data, live target data, credentialed access, or unclear provenance
Transform	summary, comparison, rubric scoring, tabletop simulation, or audit review	collection expansion, external action, or unsafe system interaction
Output	memo, matrix, checklist, ledger, rubric, or debrief packet	deployable procedure, target package, or automated action plan
Reviewer	human reviewer, approval gate, revision note, and refresh owner	anonymous ownership or no escalation path

79.1.6 Instructor Capstone, Rubric, and Red-Team Review Pack input/output contract

Section anchor. Section 79.

Contract term	Input rule	Output rule
Source identity	retain `ageintNNN`, title, URL, and checked status	cite with Pandoc keys and avoid pasted raw URLs in prose
Accessibility	include plain-language labels, table headers, and figure alternatives	reject inaccessible figures, unlabeled tables, or single-modality evidence
Rights	identify affected groups, safeguards, and residual risk	preserve privacy, equality, access, contestability, and redress notes
Tooling	use allowlisted tools, visible prompts, logs, and stop conditions	keep outputs evidence-bounded, reversible, and human-reviewed
Refresh	record source, policy, standard, incident, or assessment trigger	assign an owner and date for revalidation

79.1.7 Instructor Capstone, Rubric, and Red-Team Review Pack failure cases and required responses

Section anchor. Section 79.

Failure case	Signal	Required response
Source laundering	claim cites an agent summary instead of a verified source	rebuild the claim ledger from direct sources

Failure case	Signal	Required response
Boundary drift	exercise starts asking for live targets, private data, or external action	stop, substitute synthetic inputs, and document the block
Accessibility gap	learner cannot inspect, navigate, or complete the artifact	remediate and retest before reuse
Rights gap	affected group, safeguard, or redress path is missing	run HRIA/DPIA worksheet and escalate unresolved risk
Vendor opacity	tool owner, data use, logs, or exit path is unknown	replace tool or pause until procurement evidence exists

79.1.8 Instructor Capstone, Rubric, and Red-Team Review Pack evidence package schemas

Section anchor. Section 79.

Model and dataset card:

Field	Model card evidence	Dataset card evidence	Review gate
Intended use	accountable task, excluded uses, affected users, human reviewer, and accountable owner	Data Cards purpose statement, recommended use, prohibited reuse, stewardship owner, and affected stakeholder groups	claim is rejected if intended use, excluded use, affected users, or owner is missing
Provenance and collection	model family, version, supplier or lab, training cutoff, deployment context, and configuration hash	upstream source, collection process, annotation method, consent or authority basis, sensitivity class, and license	artifact is held if provenance, license, authority, or collection process is opaque
Composition and limits	capability boundary, known failure modes, tool permissions, context window limits, and unsupported conditions	population, sampling frame, coverage gaps, subgroup visibility, missingness, transformations, and known caveats	artifact is revised if population, coverage, or source limits are invisible
Evaluation and caveats	benchmark suite, task-specific tests, subgroup or context results, red-team findings, uncertainty notes, and failure examples	quality tests, label agreement, bias review, measurement limits, transformation log, and Data Cards answer-evaluation notes	empirical or performance claims are rejected unless test context, subgroup caveats, and uncertainty are visible
Lifecycle controls	release gate, rollback path, monitoring signal, incident threshold, refresh trigger, and model-card update owner	retention rule, access boundary, update cadence, deletion path, stewardship handoff, and dataset-card revision trigger	reuse is blocked without owner, retention, monitoring, rollback, and refresh evidence

Transparency notice:

Step	Artifact	Review gate
Public purpose	plain-language purpose, authority, affected service, and decision role	reader can tell why the system exists and where human judgment remains
Tool and data summary	model, data, supplier, provenance, validation, and accessibility summary	sensitive details are de-sensitized without hiding accountability fields
Impact and review	benefits, risks, safeguards, human review, appeal, and contact point	affected groups can identify recourse and oversight owners
Publication decision	publish, partially publish, delay, or hold decision with exemption rationale	non-public fields have a documented legal, security, privacy, or IP basis

Records retention and audit trail:

Record	Retained fields	Audit question
Source and prompt register	source identity, prompt version, tool allowlist, reviewer, timestamp, and caveat	Can a later reviewer reconstruct the evidentiary path without private or live data?
Decision and exception log	risk owner, accepted exception, compensating control, expiry date, and approval	Is every deviation time-bound, justified, and reviewable?
Artifact retention note	output type, sensitivity, access boundary, deletion rule, and refresh trigger	Does the retention choice match the educational purpose and rights impact?
Incident and remediation record	incident signal, containment action, root cause, owner, retest result, and closure date	Can the same failure be detected and prevented in the next reuse cycle?

Release and change-control gate:

Gate	Release evidence	Block condition
Scope freeze	accountable use case, excluded actions, tool profile, and data boundary	scope expands to external action, live data, or an unreviewed capability
Security and rights review	privacy, accessibility, security, bias, and human-review checks	rights impact, vulnerability, or accessibility issue has no owner
Version and rollback	model or prompt version, changelog, test fixture, and rollback path	change cannot be reproduced, compared, or reverted
Post-release monitoring	monitoring signal, incident threshold, refresh trigger, and owner	deployment or reuse occurs without logging and retest commitments

Risk exception memo:

Field	Minimum content	Approval rule
Exception requested	what requirement cannot be met, why, affected groups, and duration	exception must be specific, time-bound, and tied to a compensating control
Risk basis	likelihood, impact, evidence, uncertainty, alternatives, and rejected options	unsupported confidence or missing alternatives returns the memo for revision
Compensating control	human review, monitoring, access limit, disclosure, remediation, and owner	control must reduce risk without creating an operational workaround

Expiry and retest	expiry date, retest condition, review cadence, and closure criteria	open-ended exceptions are rejected

Learner support and accommodation plan:

Need	Support	Evidence
Access and modality	captions, alt text, keyboard path, plain-language summary, and structured tables	accessibility checklist, defect log, and retest result
Cognitive load	worked examples, staged release, glossary, checklist, and optional practice fixture	UDL design note and learner feedback record
Assessment fairness	allowed-tool statement, AI-use declaration, alternative submission mode, and transparent rubric	assessment-integrity note and accommodation record
Feedback and remediation	revision path, office-hour prompt, example correction, and due-date flexibility policy	feedback log and instructor disposition

Instructor question bank:

Question type	Prompt	Evidence
Source challenge	Which claim would fail if the strongest source were removed or downgraded?	claim ledger revision and source-lane note
Boundary challenge	Where could this exercise drift from analysis into action, and what safe substitute prevents it?	safe-substitution decision and excluded-action card
Rights challenge	Which affected group, accessibility need, privacy interest, or redress path is under-specified?	HRIA/DPIA update and accommodation note
Assurance challenge	What failure would the current evaluation miss, and what retest would reveal it?	adversarial assurance retest and remediation owner

Remediation backlog:

Backlog item	Trigger	Closure evidence
Unverified claim	claim lacks a guide citation or directly verified anchor	verified source, removed claim, or explicit source-guide context note
Unsafe phrasing	wording implies live targeting, external action, exploitation, manipulation, or unsafe control	safe substitute, blocked context, and reviewer sign-off
Accessibility defect	artifact cannot be inspected through an expected assistive or alternative workflow	defect fix, alternative means, and retest result
Assurance gap	evaluation, release, exception, incident, or vendor evidence is incomplete	owner, due date, retest, and accepted disposition

79.1.9 Instructor Capstone, Rubric, and Red-Team Review Pack rubric scoring bands

Section anchor. Section 79.

Band	Evidence standard	Disposition
4 - ready	source identity, accessibility, rights, safety, and reviewer evidence are complete	may be reused after normal refresh review
3 - revise	one evidence field is incomplete but risk is bounded and remediable	revise before reuse
2 - hold	multiple evidence fields are incomplete or ownership is unclear	hold for instructor and assurance review
1 - reject	unsafe action, private data, inaccessible artifact, or unverified claim appears	reject and rebuild from safe inputs

79.1.10 Instructor Capstone, Rubric, and Red-Team Review Pack refresh evidence

Section anchor. Section 79.

Evidence item	Refresh trigger	Retained support
Source lane	official source, standard, or legal text changes	checked-as-of date and source note
Safety treatment	operational wording or unsafe motif appears	safe-substitution decision and blocked context
Accessibility	WCAG, UDL, or institutional accessibility duty changes	defect log, retest result, and owner
Rights	privacy, human-rights, public transparency, or education guidance changes	HRIA/DPIA revision note
Vendor/tool	contract, data-use, incident, or model capability changes	procurement packet and incident review

79.1.11 Instructor Capstone, Rubric, and Red-Team Review Pack validation rubric

Section anchor. Section 79.

Criterion	Passing evidence
Source identity	existing `ageintNNN` keys remain stable or new references are append-only
Verification	official, standards, public-domain, or scholarly URL is checked directly
Safety	method is converted into tabletop, audit, governance, or synthetic-data treatment
Reproducibility	another reviewer can rebuild the artifact from retained inputs
Rights review	privacy, IP, human-rights, workforce, and education impacts are considered where relevant

79.1.12 Instructor Capstone, Rubric, and Red-Team Review Pack debrief protocol and reuse decision

Section anchor. Section 79.

Debrief by naming what the artifact can support, what it does not establish, what source changed, what risk was avoided by safe substitution, what human approval is still required, and when the appendix should be refreshed for Capstone authorization card: learning question, allowed inputs, excluded actions, human oversight, and stop conditions; Instructor rubric for source quality, analytic rigor, agent control, rights mapping, reproducibility, and safe substitution.

79.2 Instructor capstone workflow

Section anchor. Section 79.

The instructor capstone, rubric, and red-team review pack binds each student artifact to source verification, safe substitution, rights review, assurance, and debrief evidence.

Phase	Artifact	Review gate
Question	accountable learning question and excluded-action list	instructor confirms scope, allowed data, and rights impact
Source canon	source-lane map with guide citations, verified anchors, and refresh dates	citation keys resolve and source identity lock remains stable
Evidence ledger	claim, evidence, uncertainty, confidence, and reviewer register	every material claim has a source, caveat, and owner
Safe lab	synthetic or public dataset packet, tool allowlist, and stop conditions	no live target, private data, external action, or unsafe cyber-physical step
Assurance	evaluation rubric, failure-mode drill, rights map, and remediation note	human reviewer signs off before presentation or reuse
Debrief	capstone memo with lessons, residual risk, refresh triggers, and handoff owner	all unresolved questions and future approvals are explicit

79.3 Safe artifact rows

Section anchor. Section 79.

Source motif	Unsafe source motif	Safe curriculum substitute	Blocked context
AGEINT patterns	raw source motifs can imply autonomous tasking, monitoring, response, or deception	identity-preserving pattern registry plus tabletop, audit, provenance, and governance exercises	deployment, live target tasking, or external action
OSINT tools	broad scraping, exposed-service lookup, credentialed search, or identity exposure	tool-governance audit over instructor-provided records, toy inputs, and source-quality cards	live collection expansion or private-data discovery
GEOINT	facility assessment, force assessment, geolocation targeting, or pattern-of-life inference	provided imagery metadata quality audit with synthetic change examples and uncertainty notes	live facility assessment or tracking
SOC and CTI	autonomous response, exploitability claims, indicator publishing, or production-system action	fabricated-alert tabletop triage with ATT&CK mapping, severity rationale, and debrief evidence	production containment, exploitation, scanning, or blocking
HUMINT and CI	persona construction, contact handling, elicitation, deception, or source exposure	synthetic identity-and-provenance ethics audit with role-play records and review rubrics	impersonation, covert contact, or operational-security support
Cognitive influence	covert persuasion, microtargeting, audience manipulation, or intervention delivery	opt-in media-literacy lesson plan using synthetic materials and transparent prebunking labels	campaign design or audience-targeted persuasion
ICS and OT	facility monitoring, control action, safety-system interference, or cyber-physical response	owned-lab or synthetic process-safety tabletop with logs, rollback, and human approval gates	real plant operations, live devices, or unsafe control changes

79.4 Assessment lifecycle evidence

Section anchor. Section 79.

Control	Student evidence	Instructor check
Accountable AI use	tool-use declaration and prompt/output appendix	AI assistance is allowed, visible, bounded, and aligned with the assignment
Independent reasoning	assumptions, alternatives, uncertainty, and confidence statement	student judgment is separable from agent-generated drafting
Citation integrity	source spine, verified anchors, and claim ledger	claims are not source-laundered through agent prose
Synthetic lab boundary	allowed-inputs card, excluded actions, and stop conditions	activity remains public, benign, owned-lab, synthetic, defensive, and reversible
Feedback and revision	rubric self-score, reviewer notes, and remediation log	revision evidence addresses the actual deficiency before reuse

79.5 Adversarial review evidence

Section anchor. Section 79.

Stage	Challenge question	Artifact
Misuse case	How could the module be misread as operational, unfair, inaccessible, or overconfident?	misuse-case card and safe-substitution decision
Control challenge	Which authority, data, tool, rights, or review control would fail first?	control challenge matrix
Evidence attack	Can a claim survive source verification, provenance review, and counter-evidence?	challenged claim ledger
Incident rehearsal	What happens if an agent drifts, leaks context, fabricates support, or requests unsafe action?	synthetic incident drill and recovery note
Remediation	Which wording, workflow, source, figure, or assessment gate must change before reuse?	owner, due date, retest result, and refresh trigger

79.5.1 Instructor Capstone, Rubric, and Red-Team Review Pack visual navigation and evidence figures: purpose, source flow, and limits

The appendix uses Figure 163, Figure 164, Figure 165, Figure 166, Figure 167, Figure 168, Figure 169, Figure 170, Figure 171, and Figure 10 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 78, Section 80.

79.5.2 Instructor Capstone, Rubric, and Red-Team Review Pack runtime item map and source roster: generated rows and citation support

Safe curriculum treatment	Blocked source motif, audit-only	Allowed fixture	Rejected action	Required artifact	Citation spine
I.1 Capstone authorization card: learning question, allowed inputs, excluded actions, human oversight, and stop conditions	no blocked motif; source title used verbatim	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	[242, 2026]; [243, 2026]; [246, 2026]
I.2 Instructor rubric for source quality, analytic rigor, agent control, rights mapping, reproducibility, and safe substitution	no blocked motif; source title used verbatim	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	[237, 2026]; [242, 2026]; [238, 2026]
I.3 Red-team review checklist for source laundering, automation bias, boundary drift, overconfident synthesis, and unreproducible handoff	no blocked motif; source title used verbatim	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	[235, 2026]; [236, 2026]; [272, 2026]
I.4 Safe artifact packet: source-lane map, claim ledger, synthetic lab packet, interface contract, assessment lifecycle, and debrief memo	no blocked motif; source title used verbatim	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	[258, 2026]; [266, 2026]; [271, 2026]
I.5 Capstone debrief protocol that names residual uncertainty, rights impact, refresh owner, revision plan, and approvals required before reuse	no blocked motif; source title used verbatim	public sources, synthetic records, owned-lab notes, and instructor handouts	external action, private-data processing, unsafe system interaction, or deployment	claim ledger, safe-lab packet, and reviewer handoff	[239, 2026]; [240, 2026]; [264, 2026]

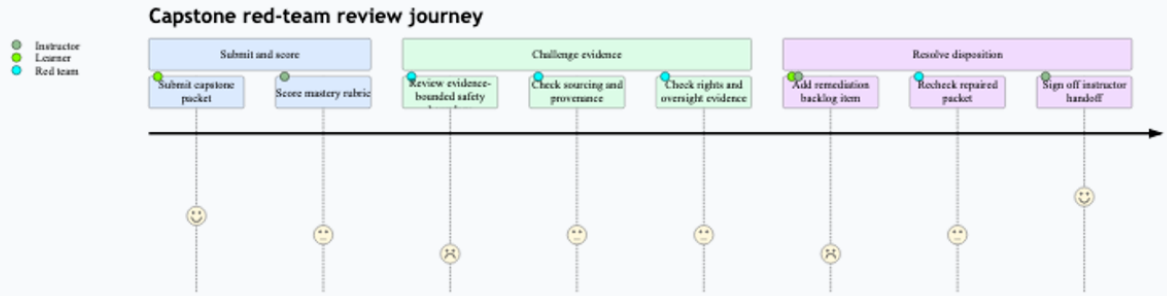


Figure 163: The capstone journey shows the reviewer experience from packet submission through rubric scoring, safety/source/rights challenge, remediation, and final instructor handoff. In the instructor capstone rubric and red team review pack appendix, it lets readers compare learner submits packet, instructor scores mastery rubric, red team checks safety, sourcing, and rights, and weak evidence enters remediation backlog so the visual functions as a traceable course aid rather than an unscoped assertion.

Figure 164: The capstone workflow moves from an accountable question to debrief and refresh ownership. Its reader value is to make capstone workflow steps, decision gates, owner handoffs, refresh triggers, and closure evidence visible at a glance, with the instructor capstone rubric and red team review pack appendix as the source section and defensive review as the boundary.

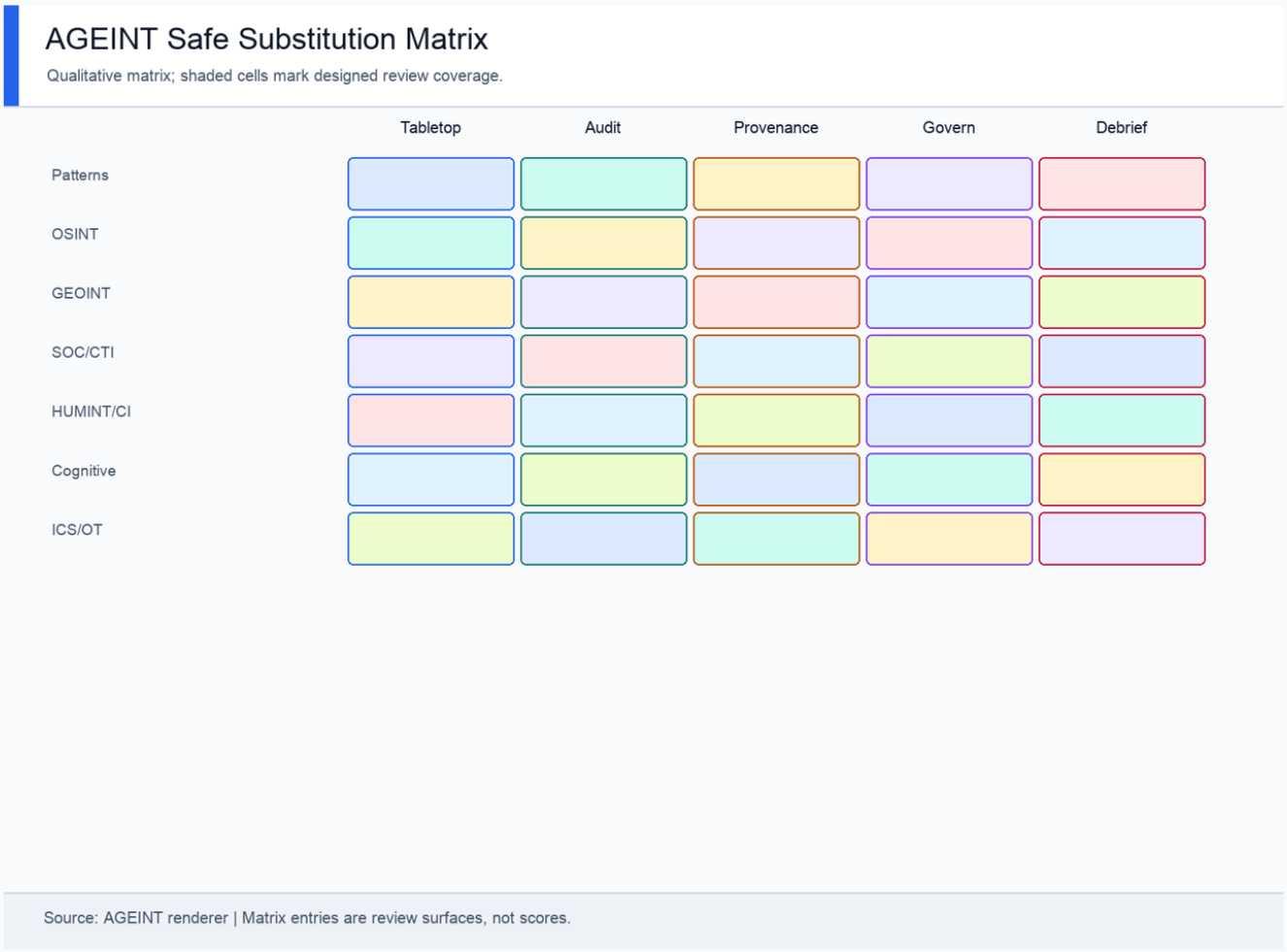


Figure 165: The safe substitution matrix converts risky motifs into bounded classroom alternatives. It is anchored to the instructor capstone rubric and red team review pack appendix; use it to inspect safe substitution matrix fields, row and column obligations, source records, reviewer decisions, and closure evidence while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

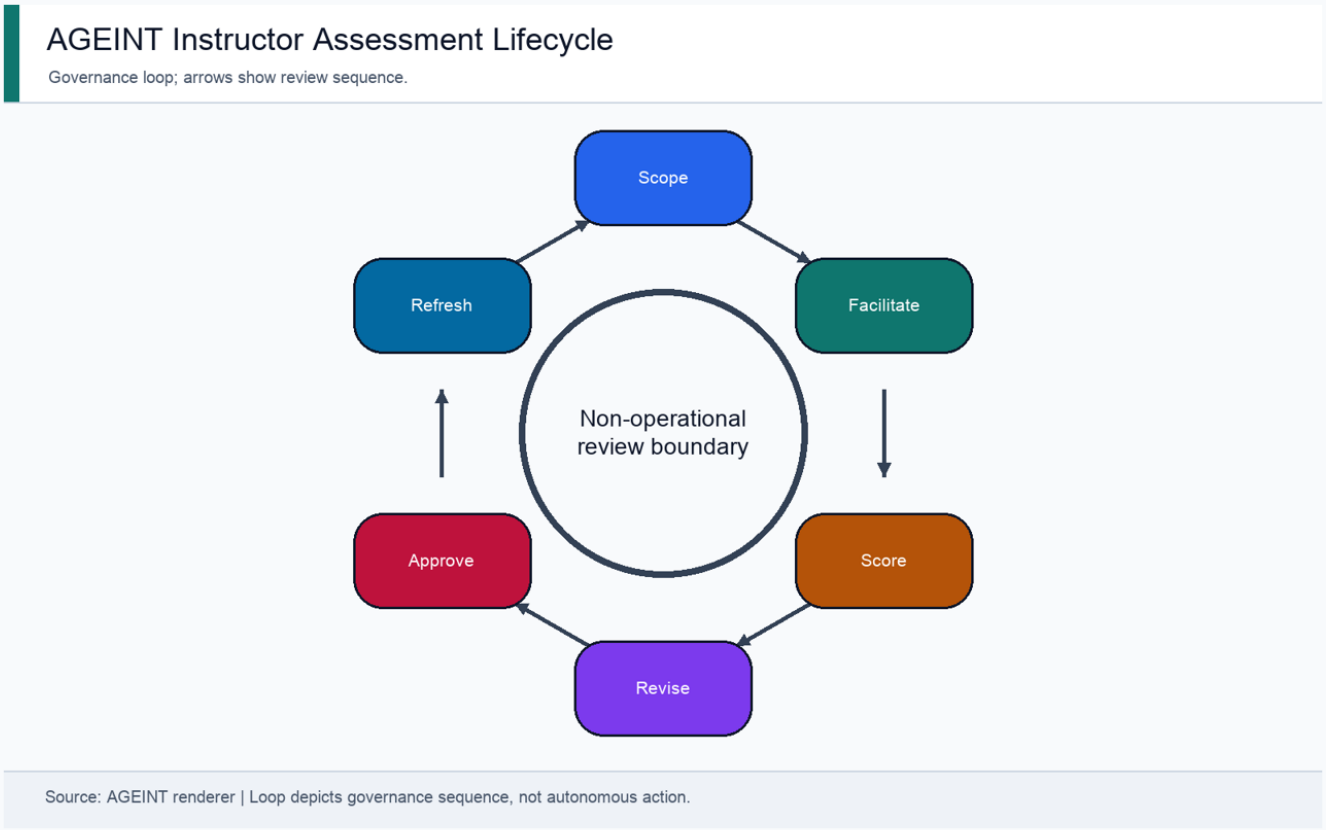


Figure 166: The instructor lifecycle connects scope, facilitation, scoring, revision, and debrief evidence. Its reader value is to make instructor assessment lifecycle steps, decision gates, owner handoffs, refresh triggers, and closure evidence visible at a glance, with the instructor capstone rubric and red team review pack appendix as the source section and defensive review as the boundary.

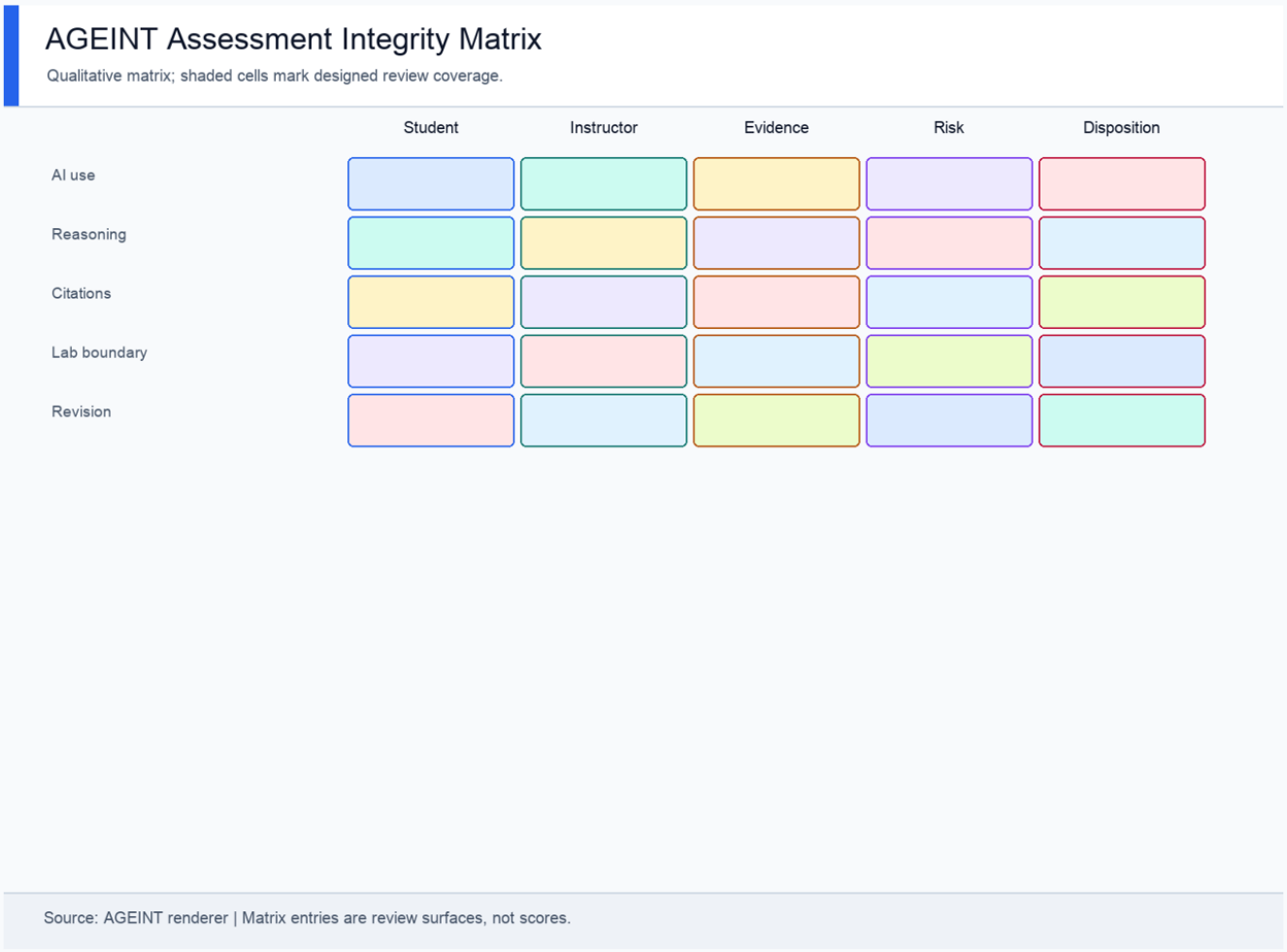


Figure 167: The assessment integrity matrix separates AI-use declarations, reasoning, citations, lab boundaries, and revision evidence. In the instructor capstone rubric and red team review pack appendix, it lets readers compare assessment integrity matrix fields, row and column obligations, source records, reviewer decisions, and closure evidence so the visual functions as a traceable course aid rather than an unscoped assertion.

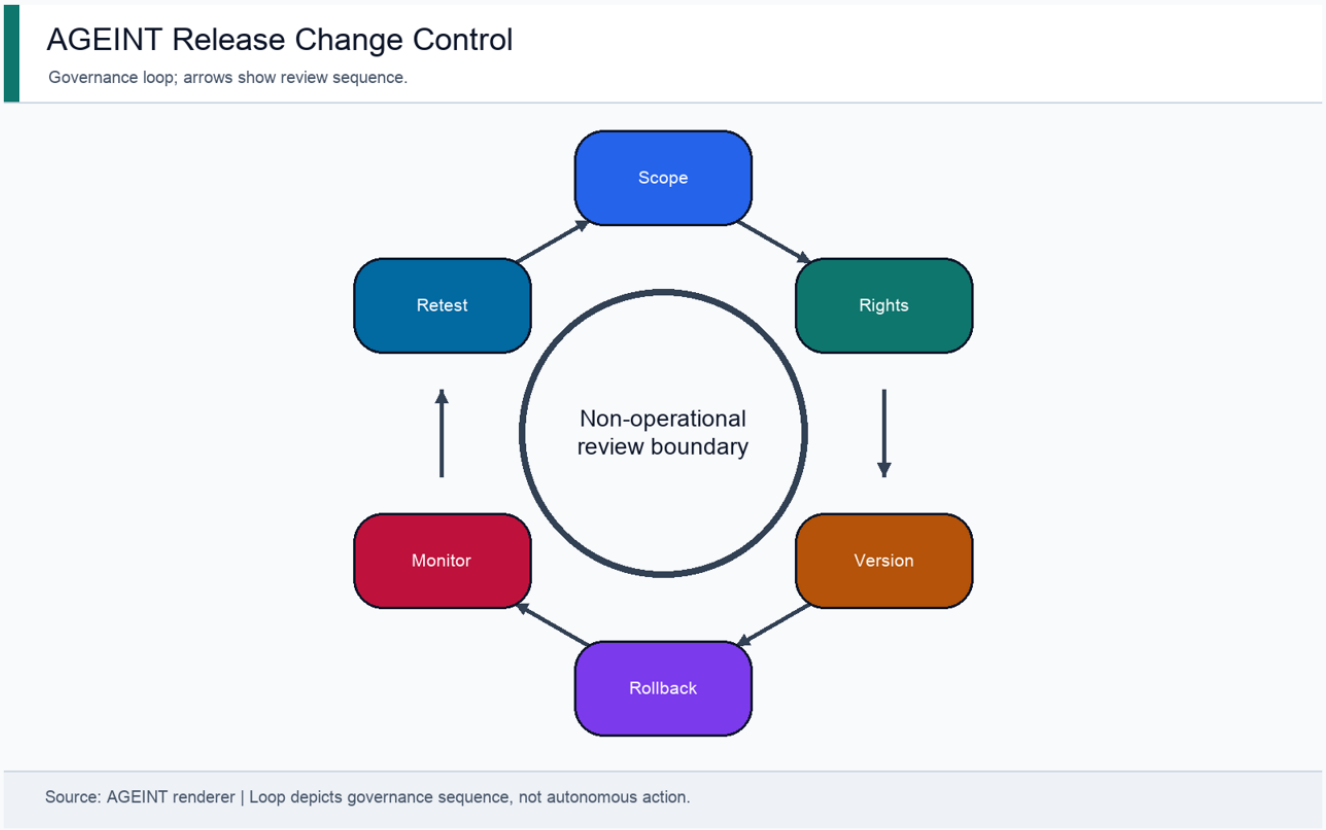


Figure 168: The release change-control gate checks scope, rights, security, versioning, rollback, monitoring, and retest. The captioned view belongs to the instructor capstone rubric and red team review pack appendix and should be read as a map of release change control labels, source records, review gates, refresh cues, and reader-use boundaries, not as a capability score or live-task instruction.

Figure 169: The learner-support plan connects access, cognitive load, assessment fairness, and remediation. It is anchored to the instructor capstone rubric and red team review pack appendix; use it to inspect learner support plan labels, source records, review gates, refresh cues, and reader-use boundaries while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

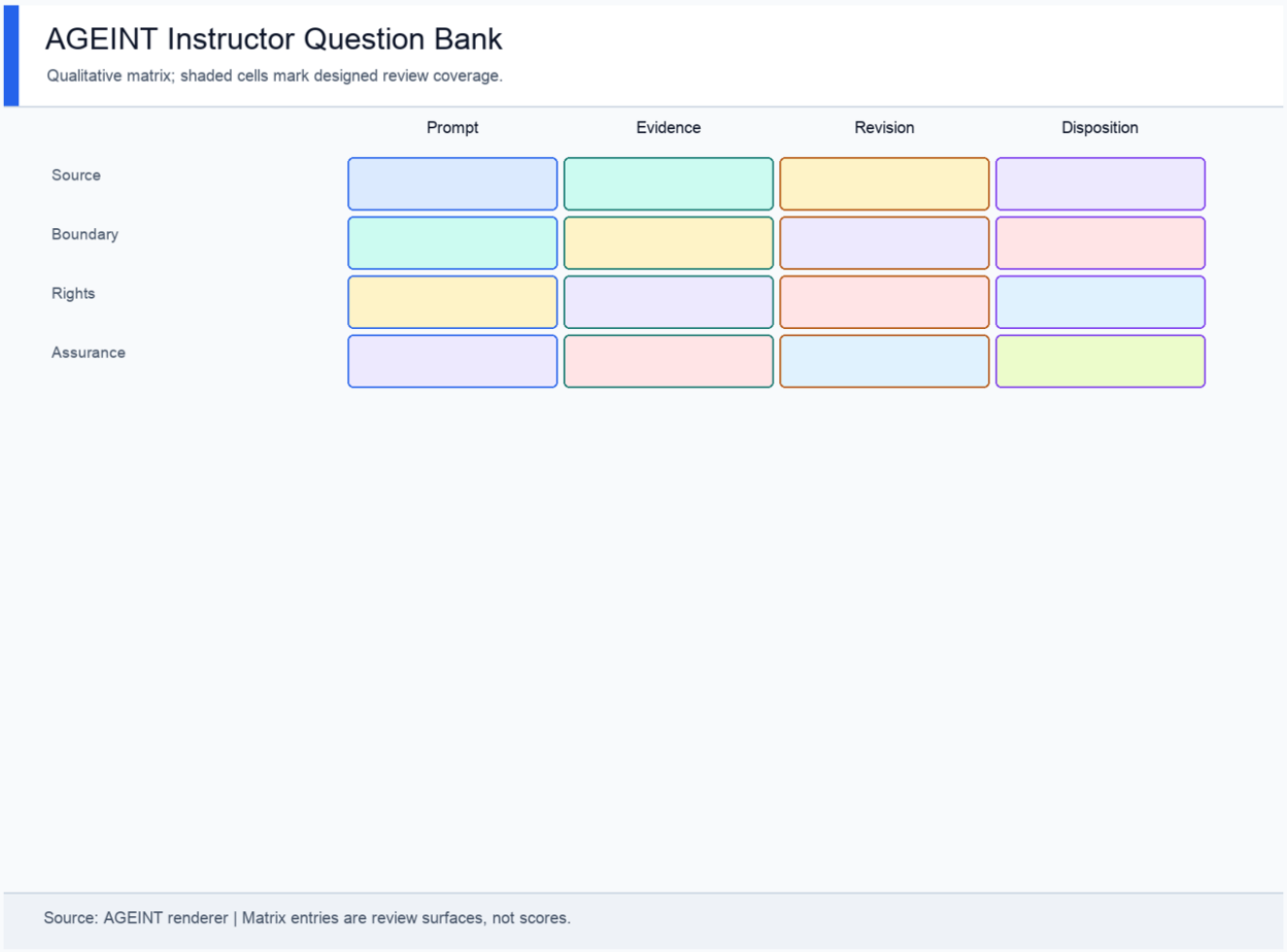


Figure 170: The instructor question bank prompts source, boundary, rights, and assurance challenges. It is anchored to the instructor capstone rubric and red team review pack appendix; use it to inspect instructor question bank fields, row and column obligations, source records, reviewer decisions, and closure evidence while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

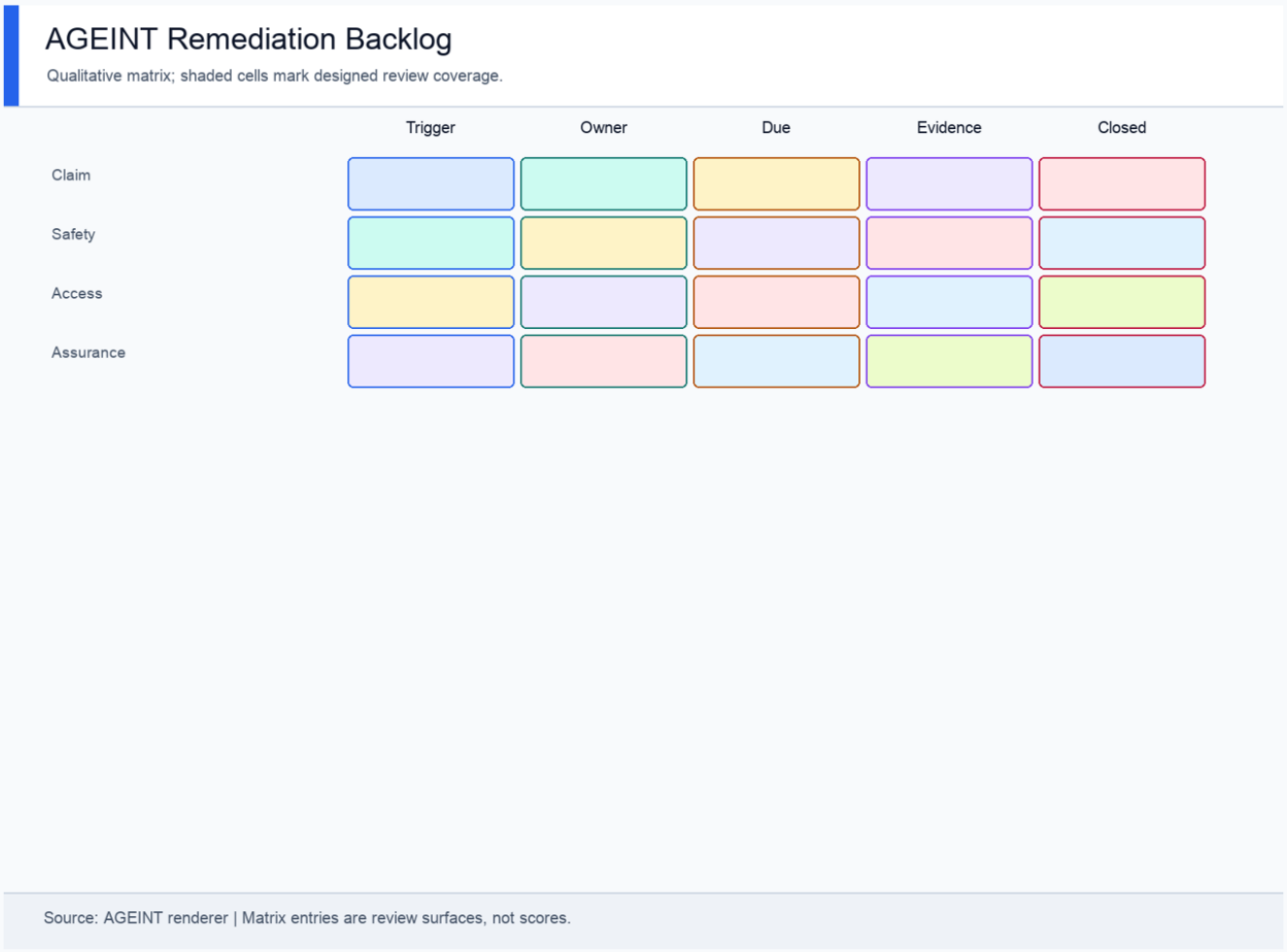


Figure 171: The remediation backlog tracks unverified claims, unsafe phrasing, accessibility defects, and assurance gaps. Its reader value is to make remediation backlog fields, row and column obligations, source records, reviewer decisions, and closure evidence visible at a glance, with the instructor capstone rubric and red team review pack appendix as the source section and defensive review as the boundary.

80 Bibliography Atlas: source keys, refresh evidence, and citation workflow

The bibliography atlas is generated from the parsed source-guide reference list plus official source-quality anchors. Citation keys are cited in prose with Pandoc citations. Treat this appendix as the source-audit surface: each curated anchor keeps its source URL, source lane, checked date, refresh trigger, and verification note visible so moved pages, blocked automated fetches, and volatile standards can be reviewed without changing citation keys.

80.1 Bibliography atlas navigation figures and source links: visual route through citation evidence

The bibliography appendix uses Figure 172, Figure 173, Figure 174, Figure 175, Figure 176, and Figure 177 to map its evidence flow, safety boundaries, review artifacts, and refresh cues.
Navigation links: Section 2, Section 79.

Figure 172: Compact audit matrix listing official source-quality anchors, their source tier, claim role, evidence use, and refresh duty; it is a source-management view, not quantitative evidence. It is anchored to the bibliography atlas; use it to inspect source quality spine categories, denominators, evidence lanes, limitations, and reviewer-use cautions while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

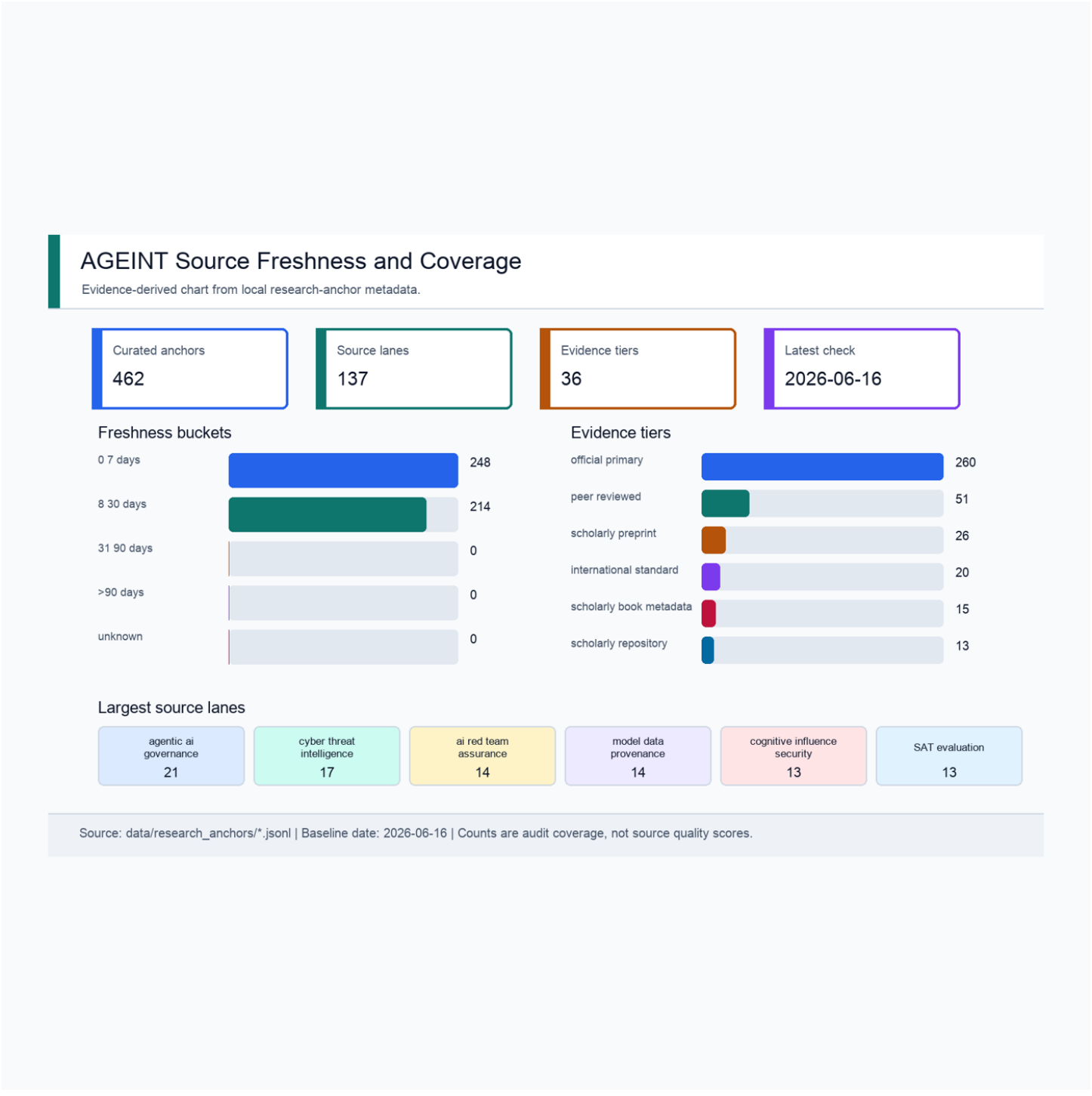


Figure 173: Evidence-derived chart summarizing curated research-anchor freshness, source lanes, and evidence tiers from local metadata; counts are audit coverage signals, not source-quality scores. In the bibliography atlas, it lets readers compare source freshness coverage categories, denominators, evidence lanes, limitations, and reviewer-use cautions so the visual functions as a traceable course aid rather than an unscoped assertion.

Figure 174: Audit table defining heterogeneous count types: parsed source-guide references, curated research anchors, methods appendices, and named AGEINT patterns. In the bibliography atlas, it lets readers compare reference coverage categories, denominators, evidence lanes, limitations, and reviewer-use cautions so the visual functions as a traceable course aid rather than an unscoped assertion.

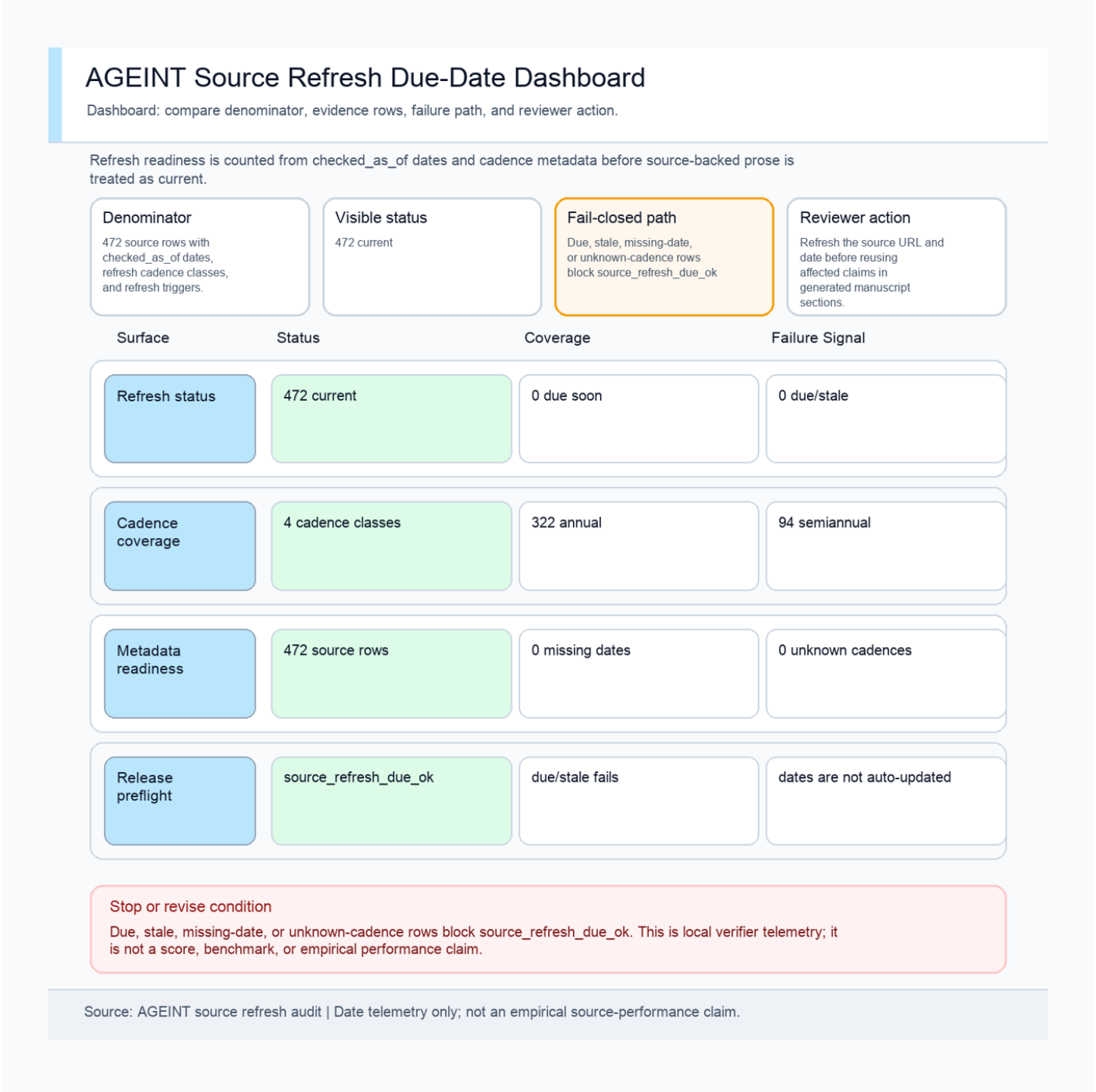


Figure 175: The source refresh due-date dashboard turns checked_as_of dates and refresh cadence metadata into a release-readiness control. It separates the 472-row local source denominator, current anchors, due-soon rows, due or stale rows, cadence coverage, missing metadata, reviewer refresh actions, and the publication-preflight failure path so source dates cannot silently age past their review window while citation, link, figure, and PDF validators remain green. The visual is not a score or empirical performance claim.

Figure 176: The agency-source coverage figure summarizes the official US Intelligence Community source expansion as agency-source coverage telemetry, not an endorsement or source-quality score. It shows the 56-anchor denominator for the new official US IC tranche, the CIA, DIA, ODNI, Intelligence.gov, NSA, NGA, FBI, and NRO agency distribution, deterministic source-pack routing into profiles, reviewer routing actions, and the artifact-evidence failure path that blocks a new agency anchor when source_agency, source_pack, source_lane, source_tier, checked_as_of, claim_scope, assurance_use, or rights_dimension metadata is missing.

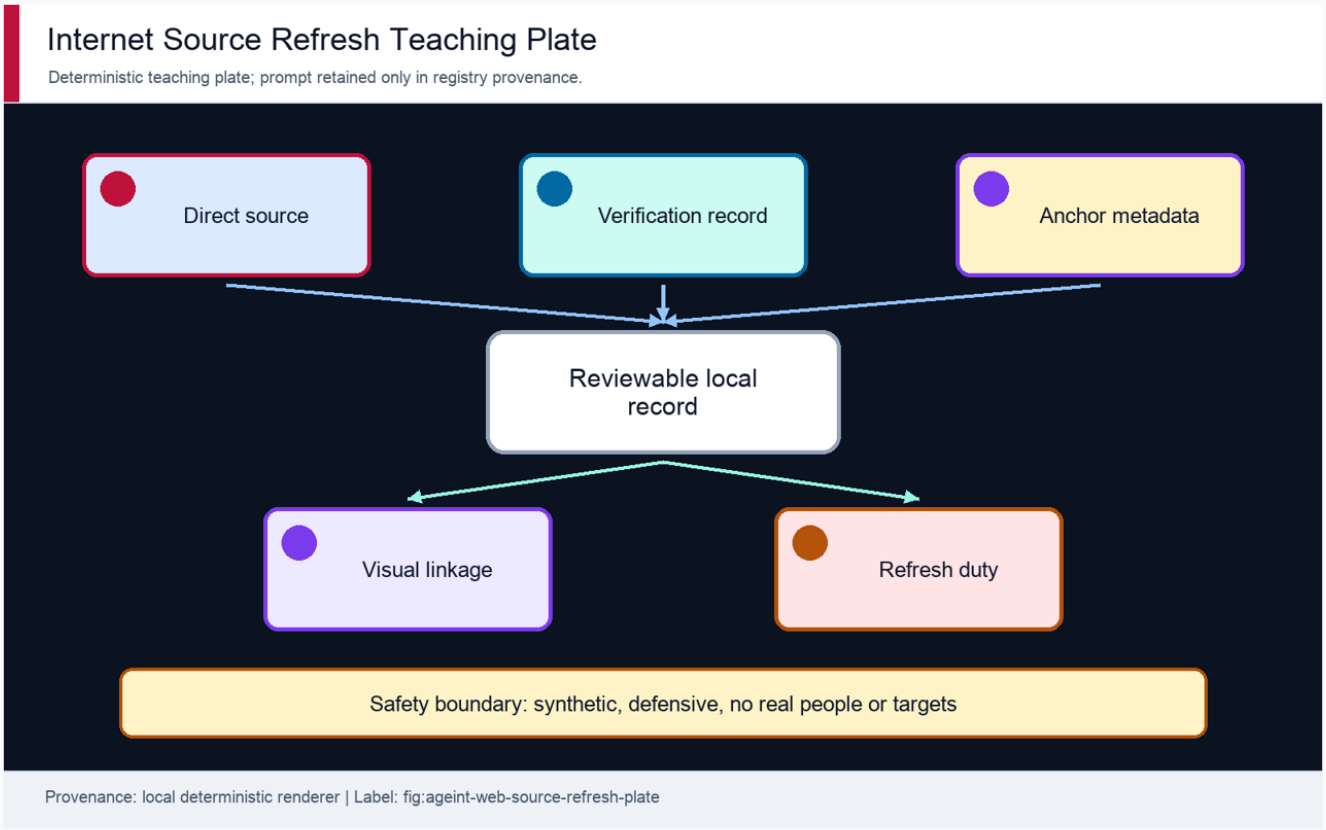


Figure 177: Deterministic teaching plate showing how web-discovered sources enter AGEINT only after direct verification, anchor metadata, figure linkage, and reviewer refresh duty. It is anchored to the bibliography atlas; use it to inspect Direct source, Verification record, Anchor metadata, and Visual linkage while preserving the distinction between curriculum structure, evidence boundary, and accountable practice.

80.2 Current-source additions and refreshes: newly checked anchors and changed caveats

The current-source table isolates anchors added or materially refreshed in the latest internet-citation pass. It is deliberately narrower than the full ledger: rows appear here only when the source URL was verified for this pass, a moved URL was refreshed, or a retrieval caveat changed the claim boundary. Draft sources retain draft-status caveats rather than being treated as final guidance.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[Jr., 2007]	Psychology of Intelligence Analysis	analytic_tradecraft	curriculum grounding and source-backed synthesis	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use; URL refreshed 2026-06-06 after liveness check.
[of Standards and Technology, 2026c]	AI Agent Standards Initiative	agent_interoperability_standards	AI agent interoperability, secure delegation, agent identity, standards gaps, protocol coordination, and evaluation research for autonomous digital actors	Direct NIST source URL verified live 2026-06-11; page identifies the AI Agent Standards Initiative as focused on trusted, interoperable, and secure agentic AI.
[Project, 2026b]	OWASP Top 10 for Agentic Applications for 2026	agentic_ai_security	Peer-reviewed OWASP security-risk taxonomy for autonomous and agentic AI applications, including agent-goal hijack, tool misuse, privilege abuse, supply-chain exposure, and inter-agent communication risk	Direct OWASP GenAI Security Project resource verified live 2026-06-11 with the 2026 Agentic Applications Top 10 scope and peer-reviewed security-risk framing.
[MITRE, 2026a]	MITRE ATLAS	ai_red_team_assurance	Adversarial Threat Landscape for Artificial-Intelligence Systems tactics, techniques, mitigations, and case-study vocabulary for defensive AI security analysis	Direct MITRE ATLAS source URL verified live 2026-06-11; page identifies ATLAS as a globally accessible living knowledge base of adversary tactics and techniques against AI systems.
[UNESCO, 2024]	AI Competency Frameworks for Teachers and Students	education_assessment	teacher facilitation, learner competencies, assessment design, and AI literacy outcomes	Direct source URL verified against an official UNESCO source for AGEINT curriculum use as of 2026-05-22; automated liveness sweep on 2026-06-06 found the old article URL moved and recorded this likely successor URL, but UNESCO reset automated retrieval, so manual browser re-verification remains required.
[Observatory, 2026b]	AI in the Public Sector	public_sector_agentic_ai	public-sector AI adoption, accountability, service design, and institutional capacity	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use; URL refreshed 2026-06-06 after liveness check.
[Observatory, 2026a]	AI and Work	workforce_governance	workforce transition, skills, productivity, workplace governance, and responsible adoption	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use; URL refreshed 2026-06-06 after liveness check.
[of Standards and Technology, 2026h]	NIST Big Data Interoperability Framework	model_data_provenance	data interoperability, architecture vocabulary, data lifecycle, and provenance-aware systems	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use; URL refreshed 2026-06-06 after liveness check.
[for Content Provenance and Authenticity, 2026]	C2PA Specifications	model_data_provenance	content provenance, authenticity metadata, media evidence, and chain-of-custody discussion	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use; URL refreshed 2026-06-06 after liveness check.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[of Standards and Technology, 2024e]	Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile	assurance_evaluation_evidence	Generative-AI risk profile, AI RMF implementation actions, evaluation controls, misuse-risk review, and trustworthiness evidence mapping	Direct NIST AI 600-1 PDF and NIST publication landing page verified live 2026-06-11 for GenAI Profile scope and AI RMF alignment.
[Cybersecurity et al., 2025b]	AI Data Security: Best Practices for Securing Data Used to Train and Operate AI Systems	model_data_provenance	AI data security for data used to train, test, deploy, and operate AI systems, including provenance, integrity, confidentiality, lifecycle controls, and trustworthy AI outcomes	Direct official CISA/NSA/FBI partner PDF verified live 2026-06-11; executive summary covers AI data security, lifecycle stages, integrity risks, and best practices.
[of Standards and Technology, 2024b]	Reducing Risks Posed by Synthetic Content: An Overview of Technical Approaches to Digital Content Transparency	model_data_provenance	Synthetic-content provenance, watermarking, labeling, detection, testing, auditing, maintenance, disclosure, and digital content transparency for generated media and influence-risk review	Direct NIST AI 100-4 PDF and publication landing page verified live 2026-06-11; report covers provenance, labeling, watermarking, detection, testing, auditing, and maintenance.
[of Standards and Technology, 2024c]	A Plan for Global Engagement on AI Standards	ai_conformity_compliance	global AI standards engagement, standards-development coordination, AI governance interoperability, and conformity-assessment planning	Direct source URL verified live (HTTP 200 PDF, title metadata and first pages on-topic) for AGEINT curriculum use.
[U.S. AI Safety Institute and Technology, 2024]	Managing Misuse Risk for Dual-Use Foundation Models, NIST AI 800-1 Initial Public Draft	ai_red_team_assurance	dual-use foundation-model misuse-risk management, safeguards, evaluation planning, governance roles, and draft-status caveats for frontier-model assurance	Direct source URL verified live (HTTP 200 PDF, title metadata and first pages on-topic); Draft status retained explicitly for AGEINT curriculum use.
[Group and Panel, 2026]	International AI Safety Report 2026	assurance_evaluation_evidence	international advanced-AI safety evidence, risk-taxonomy synthesis, capability and impact assessment, and policy-neutral scientific uncertainty framing	Direct official report landing page verified live (HTTP 200, International AI Safety Report 2026 page on-topic); the official PDF and arXiv record remain secondary evidence when needed.
[Project, 2025c]	Specification - Model Context Protocol	agent_interoperability_standards	Model Context Protocol specification, client-server-tool interoperability, capability negotiation, authorization boundaries, and agentic context integration assumptions	Direct official MCP specification page verified live 2026-06-11; security and trust language retained as a boundary, not a deployment guarantee.
[Project, 2025b]	Security Best Practices - Model Context Protocol	secure_release_change_control	MCP security best practices, confused-deputy and token-passthrough risks, human consent, least privilege, authorization boundaries, and agent-tool threat modeling	Direct official MCP security best-practices page verified live 2026-06-11; page describes security considerations, attack vectors, and best practices for MCP implementations.
[Project, 2025a]	Agent2Agent (A2A) Protocol	agent_interoperability_standards	Agent2Agent protocol interoperability, agent discovery and communication, cross-agent collaboration, and secure multi-agent coordination assumptions	Direct source URL verified live (HTTP 200, official A2A protocol documentation with on-topic description metadata) for AGEINT curriculum use.
[Centre and international partners, 2024]	Guidelines for Secure AI System Development	secure_release_change_control	secure AI system development across design, development, deployment, operation, supply-chain security, and provider-customer responsibility boundaries	Direct source URL verified live (HTTP 200, on-topic NCSC secure-AI-development guidance page) for AGEINT curriculum use.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[MITRE, 2026d]	D3FEND Matrix	assurance_evaluation_evidence	defensive cybersecurity countermeasure taxonomy, relationships between defensive techniques and adversary techniques, and evidence-backed control selection	Direct source URL verified live (HTTP 200, official MITRE D3FEND page with on-topic title and description metadata) for AGEINT curriculum use.
[Open, 2022]	Common Security Advisory Framework Version 2.0	records_retention_auditability	machine-readable security advisories, vulnerability disclosure structure, product status, remediation metadata, and advisory exchange governance	Direct canonical OASIS OS HTML source URL verified live (HTTP 200, CSAF Version 2.0 OASIS Standard page on-topic) for AGEINT curriculum use.
[Project, 2026a]	CycloneDX Specification Overview	model_data_provenance	software bill of materials, service and operations BOMs, vulnerability and dependency metadata, and supply-chain component provenance	Direct source URL verified live (HTTP 200, official CycloneDX specification overview page) for AGEINT curriculum use.
[SPDX Project, 2024]	SPDX Specification 3.0.1	model_data_provenance	software bill of materials, package and file metadata, licensing provenance, security and lifecycle profiles, and machine-readable supply-chain documentation	Direct source URL verified live (HTTP 200, official SPDX Specification 3.0.1 page with SBOM description metadata) for AGEINT curriculum use.
[of Standards and Technology, 2026j]	OSCAL - Open Security Controls Assessment Language	records_retention_auditability	machine-readable security controls, assessment plans/results, system security plans, component definitions, and compliance evidence exchange	Direct source URL verified live (HTTP 200, official NIST OSCAL page) for AGEINT curriculum use.
[chain Levels for Software Artifacts Project, 2026]	SLSA Specification	secure_release_change_control	supply-chain security levels, build provenance, artifact integrity, dependency risk, and incremental release-control guarantees	Direct source URL verified live (HTTP 200, official SLSA v1.1 specification page with on-topic description metadata) for AGEINT curriculum use.
[in-toto Project, 2026]	in-toto	secure_release_change_control	software supply-chain layout, signed attestations, step-level integrity, artifact provenance, and verifiable release workflow evidence	Direct source URL verified live (HTTP 200, official in-toto project page) for AGEINT curriculum use.
[Project, 2026c]	Overview - Sigstore	secure_release_change_control	software signing, transparency logs, artifact identity, provenance verification, and tamper-evident release evidence	Direct source URL verified live (HTTP 200, official Sigstore documentation overview page) for AGEINT curriculum use.
[Friston, 2010]	The free-energy principle: a unified brain theory?	cognitive_active_inference	Lesson 1 'Active Inference and AGEINT' — the claim that variational free energy bounds surprise, providing the primary source behind a treatment previously grounded in a bachelor's thesis.	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Friston, 2017]	Active Inference: A Process Theory	cognitive_active_inference	Lessons 2 & 4 — belief updating, policy selection, and expected free energy as the action-selection objective.	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Da Costa, 2020]	Active inference on discrete state-spaces: A synthesis	cognitive_active_inference	Discrete-state / POMDP modeling underpinning agentic systems in AGEINT.	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Parr, 2022]	Active Inference: The Free Energy Principle in Mind, Brain, and Behavior	cognitive_active_inference	Chapter-level foundational reference for the active inference material across the AGEINT curriculum.	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[Yao, 2023a]	ReAct: Synergizing Reasoning and Acting in Language Models	agentic_ai_governance	Backs the reason-act/tool-use design pattern, replacing a secondary blog/LinkedIn discussion with the canonical primary source.	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Shinn, 2023]	Reflexion: Language Agents with Verbal Reinforcement Learning	agentic_ai_governance	Backs the self-reflection / stop-condition design pattern for iterative LLM agents.	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Park, 2023]	Generative Agents: Interactive Simulacra of Human Behavior	agentic_ai_governance	Backs the memory/planning/multi-agent simulation design pattern.	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Wei, 2022]	Chain-of-Thought Prompting Elicits Reasoning in Large Language Models	agentic_ai_governance	Backs the reasoning-decomposition design pattern.	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Schick, 2023]	Toolformer: Language Models Can Teach Themselves to Use Tools	agentic_ai_governance	Backs the tool-use / API-calling design pattern.	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Wooldridge, 1995]	Intelligent agents: theory and practice	agentic_ai_governance	Backs the foundational agent definition and MAS vocabulary.	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Wooldridge, 2009]	An Introduction to MultiAgent Systems, 2nd Edition	agentic_ai_governance	Backs multi-agent coordination concepts and vocabulary.	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Burkett, 2013]	An Alternative Framework for Agent Recruitment: From MICE to RASCLS	counterintelligence_source_integrity	Backs the MICE-to-RASCLS recruitment-motivation framework with the original official CIA source, supplementing a secondary training-book treatment.	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Meissner, 2017]	Developing an Evidence-Based Perspective on Interrogation: A Review of the U.S. Government's High-Value Detainee Interrogation Group Research Program	counterintelligence_source_integrity	Backs the AGEINT claim that effective, evidence-based elicitation is rapport-based and rights-respecting rather than coercive.	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Brimbal, 2020]	Developing Rapport and Trust in the Interrogative Context: An Empirically Supported Alternative	counterintelligence_source_integrity	Backs the AGEINT contrast between rapport-based and coercive elicitation and its ethics/consent governance framing.	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Nunan, 2020]	Eliciting human intelligence: police source handlers' perceptions and experiences of rapport during covert human intelligence sources (CHIS) interactions	counterintelligence_source_integrity	Backs the AGEINT treatment of source-handler rapport and CHIS governance in operational HUMINT.	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Kelly, 2013]	A Taxonomy of Interrogation Methods	counterintelligence_source_integrity	Backs the AGEINT study-taxonomy framing of interrogation/elicitation methods, signaling analytic categorization rather than an operational how-to.	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[Pherson, 2014a]	Structured Analytic Techniques for Intelligence Analysis	analytic_tradecraft	Grounds the AGEINT structured-analytic-techniques (SAT) catalogue and definitions, supplying an authoritative primary anchor for the techniques enumerated in the curriculum.	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[of Standards and , NIST]	FIPS 197: Advanced Encryption Standard (AES)	cyber_threat_intelligence	Anchors the symmetric-encryption / confidentiality element of the SIGINT chapter's crypto-assurance discussion.	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[of Standards and , NIST]	FIPS 186-5: Digital Signature Standard (DSS)	cyber_threat_intelligence	Anchors the digital-signature / authentication / provenance element of the crypto-assurance figure.	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[of Standards and , NIST]	FIPS 180-4: Secure Hash Standard (SHS)	cyber_threat_intelligence	Anchors the integrity / hashing layer of the SIGINT chapter's crypto-assurance discussion.	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[, NIST]	NIST SP 800-57 Part 1 Rev. 5: Recommendation for Key Management, Part 1: General	cyber_threat_intelligence	Anchors the key-management / crypto-lifecycle governance discussion tying the cipher, signature, and hash standards into an operational regime.	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[McGuire, 1961]	Resistance to persuasion conferred by active and passive prior refutation of the same and alternative counterarguments	cognitive_influence_security	Provides the historical and mechanistic foundation for AGEINT's inoculation/prebunking claims (the modern van der Linden and Roozenbeek literature), establishing that refutational pre-exposure confers durable resistance to influence operations.	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Mahima Pushkarna and Kjartansson, 2022]	Data Cards: Purposeful and Transparent Dataset Documentation for Responsible AI	dataset_documentation	Data Cards for purposeful, stakeholder-centered dataset documentation across origins, collection, annotation, intended use, evaluation context, lifecycle changes, and responsible AI review	Direct arXiv source URL verified live 2026-06-09 with title, authors, abstract, and ACM FAccT 2022 metadata matching the cited Data Cards paper.
[Christopher L. Buckley and Seth, 2017]	The Free Energy Principle for Action and Perception: A Mathematical Review	cognitive_active_inference	Mathematical review of the free energy principle and active inference as a theory of action and perception, including variational free energy, generative models, and explicit modeling assumptions	Direct arXiv source URL verified live 2026-06-10 with title, authors, submission date, abstract, and DOI metadata matching the cited mathematical review.
[Melissa L. Rethlefsen and the PRISMA-S Group, 2021]	PRISMA-S: An Extension to the PRISMA Statement for Reporting Literature Searches in Systematic Reviews	source_construction_reporting	PRISMA-S reporting guideline for documenting literature searches, search strategies, information sources, limits, records, and reproducibility details	Direct journal landing page verified live 2026-06-10 with title, authors, publication date, journal metadata, and abstract describing the 16-item PRISMA-S checklist.
[Kai Greshake and Fritz, 2023]	Not What You've Signed Up For: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection	agentic_ai_security	Indirect prompt injection risk in LLM-integrated applications where retrieved or external content can alter model behavior and trigger data theft, tool misuse, or ecosystem contamination	Direct arXiv source URL verified live 2026-06-10 with title, authors, submission and revision metadata, DOI, and abstract describing indirect prompt-injection attacks.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[of Standards and Technology, 2026b]	Practices for Automated Benchmark Evaluations of Language Models and AI Agent Systems, NIST AI 800-2 Initial Public Draft	assurance_evaluation_evidence	Initial public draft practices for automated benchmark evaluations of language models and AI agent systems, including defining evaluation context, conducting benchmark evaluation, and communicating results	Direct NIST AI 800-2 PDF and NIST announcement verified live 2026-06-11; draft status retained explicitly for AGEINT curriculum use.
[for Economic Co-operation and Development, 2026a]	The Agentic AI Landscape and Its Conceptual Foundations	agent_interoperability_standards	OECD expert analysis of agentic AI definitions, frequently cited features, conceptual foundations, uptake trends, and mapping to the OECD AI system definition	Direct OECD publication page verified live 2026-06-11; abstract describes definition comparison, OECD AI-system mapping, and uptake trends.
[Agency, 2026i]	Model Context Protocol (MCP): Security Design Considerations for Organizations	secure_release_change_control	Official cybersecurity information sheet on Model Context Protocol security design considerations, deliberate controls beyond protocol suggestions, and secure adoption safeguards for MCP implementations	Direct NSA PDF URL verified live 2026-06-11; guidance frames MCP security adoption controls and recommendations for organizations.
[Jon Roozenbeek and Lewandowsky, 2022]	Psychological Inoculation Improves Resilience Against Misinformation on Social Media	cognitive_resilience_evidence	Peer-reviewed Science Advances study testing psychological inoculation videos for improving misinformation resilience at scale, with bounded transfer from measured outcomes to curriculum claims	Direct Science Advances DOI page verified live 2026-06-11 with title, journal, DOI, and abstract-level claim that inoculation campaigns improved misinformation resilience at scale.
[for the Study of Intelligence, 2002]	Sherman Kent and the Profession of Intelligence Analysis	analytic_tradecraft_evidence	Supports claims about Kent's role in professional analytic standards and intelligence-analysis identity.	Direct CIA PDF verified live 2026-06-11; use for Kent-as-profession and standards claims, not for contemporary agency policy.
[for the Study of Intelligence, 1994]	Sherman Kent's Final Thoughts on Analyst-Policymaker Relations	analytic_tradecraft_evidence	Supports bounded claims about analyst-policy communication and warning-intelligence responsibilities.	Direct CIA PDF verified live 2026-06-11; use for warning and analyst-policy boundary framing.
[Wohlstetter, 1962]	Pearl Harbor: Warning and Decision	warning_intelligence	Supports historical warning-intelligence claims about signal-noise and surprise analysis.	Stanford University Press publisher page verified live 2026-06-11; use as classic warning theory, not as current doctrine.
[Grabo, 1972]	Handbook of Warning Intelligence	warning_intelligence	Supports claims about indications, warning, assumptions, and uncertainty in historical warning practice.	CIA Reading Room PDF verified live 2026-06-11; use for historical warning concepts, not operational collection instructions.
[Congress, 2004]	Intelligence Reform and Terrorism Prevention Act of 2004	intelligence_failure_postmortem	Supports claims that post-9/11 reforms created statutory pressure for analytic integrity and alternative analysis.	GovInfo public law landing page verified live 2026-06-11; use for statutory reform context, not implementation-detail claims.
[on Terrorist Attacks Upon the United States, 2004]	The 9/11 Commission Report	intelligence_failure_postmortem	Supports bounded claims about post-9/11 warning and reform context.	Official commission PDF verified live 2026-06-11; use for postmortem and reform context, not as a one-size failure formula.
[on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005]	Report to the President of the United States: The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction	intelligence_failure_postmortem	Supports bounded claims about Iraq WMD intelligence failure, assumptions, evidence gaps, and analytic reform.	Defense policy-hosted official report PDF verified live 2026-06-11; use for assumptions/evidence and analytic-failure context.
[Transformation, 2017]	Alternative Analysis Handbook	analytic_tradecraft_evidence	Supports claims about alternative-analysis practice menus and facilitation, with empirical limits stated separately.	NATO ACT PDF verified live 2026-06-11; use as doctrine/practice guidance, not empirical proof of SAT effectiveness.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[Bruce, 2016]	Assessing the Value of Structured Analytic Techniques in the U.S. Intelligence Community	sat_evaluation_evidence	Supports claims that SAT effectiveness evidence is limited and requires systematic evaluation.	RAND report metadata and PDF URL verified again on 2026-06-15 from the RAND publication record and direct PDF URL; use for evaluation-limit claims and evidence-boundary framing.
[Alexandru Marcoci and Jonas, 2019]	Better Together: Reliable Application of the Post-9/11 and Post-Iraq US Intelligence Tradecraft Standards Requires Collective Analysis	sat_evaluation_evidence	Supports claims about rater reliability limits and value of collective review for tradecraft standards.	Frontiers open article verified live 2026-06-11; use for tradecraft-rating reliability and collective review claims.
[Barnes and Mandel, 2014]	Accuracy of Forecasts in Strategic Intelligence	forecasting_calibration_evidence	Supports bounded claims about strategic-intelligence forecast accuracy, calibration, discrimination, and underconfidence.	PNAS DOI/publisher page and PubMed metadata verified live 2026-06-11; use for forecast-calibration claims.
[Ard, 2024]	Structured Analytic Techniques: A Pragmatic Approach	sat_evaluation_evidence	Supports evidence-boundary claims that SATs need qualification and should not be presented as proven universal debiasing tools.	DOI metadata verified live 2026-06-15 through Crossref for title, author, and publication year; publisher URL retained because automated publisher retrieval may be rate-limited.
[Jennifer Stromer-Galley and colleagues, 2020]	Flexible Versus Structured Support for Reasoning: Enhancing Analytical Reasoning Through a Flexible Analytic Technique	sat_evaluation_evidence	Supports bounded claims that flexible SAT support can improve reasoning quality in a specific experimental setting.	University of Glasgow repository metadata verified live 2026-06-11; use for flexible-SAT evidence as one bounded study, not all-purpose SAT proof.
[Betts, 1978]	Analysis, War, and Decision: Why Intelligence Failures Are Inevitable	intelligence_failure_postmortem	Supports claims that intelligence failure often emerges from analysis-decision interaction and cannot be reduced to missing technique alone.	Cambridge Core publisher page verified live 2026-06-11; use for failure-theory context, not fatalistic claims that improvement is impossible.
[Jervis, 2022]	Why Intelligence and Policymakers Clash	intelligence_failure_postmortem	Supports claims about policy-intelligence friction, hindsight bias in postmortems, and limits of simple failure narratives.	PNAS DOI/publisher metadata verified live 2026-06-11; use for postmortem and policy-friction boundary claims.
[Wirtz, 2023]	Are Intelligence Failures Still Inevitable?	intelligence_failure_postmortem	Supports current failure-theory framing that reform can improve systems without eliminating surprise or policy-analysis friction.	DOI/publisher URL retained; scholarly metadata verified live 2026-06-11 from DOI-indexed search results because automated publisher retrieval was rate-limited.
[Central Intelligence Agency, 1993]	Words of Estimative Probability	analytic_uncertainty_language	estimative-language calibration and uncertainty-expression support, not empirical AGEINT benchmark evidence	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 1970s]	The IC's Struggle to Express Uncertainty in the 1970s	analytic_uncertainty_language	historical uncertainty-communication support and analytic-language caution	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2018b]	Developing a Taxonomy of Intelligence Analysis Variables	analytic_method_design	taxonomy and analytic-variable support for source-backed method decomposition	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Johnston, 2005]	Analytic Culture in the U.S. Intelligence Community	intelligence_profession_literature	professional-context support for analytic culture, method standardization limits, and institution-level tradecraft constraints	Direct CIA CSI book page and static PDF URL verified on 2026-06-15; metadata updated to preserve the existing citation key while crediting the monograph author.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[Central Intelligence Agency, 1955]	The Need for an Intelligence Literature	intelligence_profession_literature	professional-literature and method-governance support for Synthetic Analytic Tradecraft framing	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2025b]	Studies in Intelligence Author's Guide 2025: Guidance Section Only	intelligence_writing_and_review	professional writing and review-process support for manuscript discipline	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2025a]	Applying Epistemology to Intelligence Analysis	analytic_epistemology	epistemic-framing support for calibrated claims and reviewer challengeability	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2023]	Agile Analysis: Transforming Intelligence Production Through Lean Startup Principles	analytic_production_workflow	workflow and analytic-production support for iterative, reviewable tradecraft artifacts	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2018c]	Managing the Reliability Cycle: An Alternative Approach to Thinking About Intelligence Failure	intelligence_failure_postmortem	failure-analysis and reliability-cycle support for reviewer challenge and rollback claims	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2018f]	Why Bad Things Happen to Good Analysts	intelligence_failure_postmortem	failure-mode support for calibrated reviewer challenge and non-guarantee language	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2019]	The Future of Analysis	ai_enabled_analysis_boundary	future-analysis context for bounded AI assistance and human analytic structure, not deployed benchmark evidence	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 1999]	Psychology of Intelligence Analysis	analytic_cognition_and_bias	cognitive and analytic-judgment support for bias-aware review, not universal debiasing proof	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov; note retains CIA disclaimer context.
[Central Intelligence Agency, 1994]	Sherman Kent and the Board of National Estimates: Collected Essays	declassified_analytic_history	declassified historical support for analytic-profession and estimative-institution lessons	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2020]	Lessons from SABLE SPEAR: The Application of an Artificial Intelligence Methodology to Tactical Intelligence	ai_enabled_analysis_boundary	professional-context support for AI-assisted analysis boundaries, not AGEINT benchmark evidence	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2018a]	A Call for More Humility in Intelligence Analysis	analytic_cognition_and_bias	analytic-humility support for calibrated claims and challengeable evidence packets	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2021a]	Voice of Experience: Principles of Intelligence Analysis	analytic_method_design	professional principle support for source-backed analytic synthesis and reviewer handoff	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2018e]	War and Chance: Assessing Uncertainty in International Politics	analytic_uncertainty_language	uncertainty-language and prediction-limit context for calibrated analytic prose	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2005a]	Fifty Years of Studies in Intelligence	intelligence_profession_literature	professional-literature history for manuscript and curriculum-source governance	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2018d]	Thinking and Writing: Cognitive Science and Intelligence Analysis	intelligence_writing_and_review	writing and cognitive-science context for clearer evidence packets and analytic communication	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[Central Intelligence Agency, 2005b]	Creation of a National Institute for Analytic Methods	analytic_method_design	method-development support for verifier-first analytic substrate design	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2006]	When Everything is Intelligence - Nothing is Intelligence	intelligence_profession_literature	definition and professional-boundary support for intelligence-analysis framing	Direct URL verified on 2026-06-14 with curl HTTP 200 and text/html content from cia.gov.
[Central Intelligence Agency, 1998]	CIA and the Vietnam Policymakers: Three Episodes 1962-1968	declassified_analytic_history	declassified history support for analyst-policymaker boundary and institutional lessons	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2021b]	Intelligent Analysis: How to Defeat Uncertainty in High-Stakes Decisions	analytic_uncertainty_language	uncertainty-management context for bounded analytic-decision support language	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2017]	The Limits of Prediction - or, How I Learned to Stop Worrying About Black Swans and Love Analysis	forecasting_calibration_evidence	prediction-limit and forecasting-caution support, not evidence of AGEINT forecast accuracy	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2026]	Espionage in Our AI Future	ai_enabled_analysis_boundary	AI-era intelligence context for bounded agentic assistance and counterintelligence caution	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[of the Director of National Intelligence, 2026a]	Annual Threat Assessment of the U.S. Intelligence Community 2026	current_threat_baseline	public threat-context grounding and warning-topic baseline, not operational targeting or AGEINT benchmark evidence	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF title and content matched the Annual Threat Assessment.
[of the Director of National Intelligence, 2013a]	Intelligence Community Directive 205: Analytic Outreach	analytic_outreach_governance	analytic-outreach governance support for expert engagement and risk controls	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF title and text matched ICD 205 Analytic Outreach.
[of the Director of National Intelligence, 2008]	Intelligence Community Directive 207: National Intelligence Council	national_intelligence_governance	IC governance and national-intelligence production context	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 207.
[of the Director of National Intelligence, 2017b]	Intelligence Community Directive 208: Maximizing the Utility of Analytic Products	analytic_product_dissemination	analytic-product utility, discoverability, and dissemination-governance support	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 208.
[of the Director of National Intelligence, 2012]	Intelligence Community Directive 209: Tearline Production and Dissemination	tearlines_and_release_governance	tearline and release-governance support for public-facing evidence boundaries	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 209.
[of the Director of National Intelligence, 2013b]	Intelligence Community Directive 403: Foreign Disclosure and Release of Classified National Intelligence	foreign_disclosure_governance	foreign-disclosure governance support for release-boundary and control-marking lessons	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 403.
[of the Director of National Intelligence, 2024a]	Intelligence Community Directive 405: Intelligence Diplomacy	intelligence_diplomacy_governance	governance context for intelligence diplomacy and partner-engagement boundaries	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 405.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[of the Director of National Intelligence, 2024b]	Intelligence Community Directive 406: IC Engagement with Non-State Entities	non_state_engagement_governance	non-state engagement governance support for source, outreach, and no-tasking boundaries	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 406.
[of the Director of National Intelligence, 2024c]	Intelligence Community Directive 503: Intelligence Community Information Environment Risk Management	ic_information_environment_risk	information-environment risk governance support for secure, auditable intelligence systems	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 503.
[of the Director of National Intelligence, 2013f]	Intelligence Community Directive 900: Integrated Mission Management	integrated_mission_management	mission-management governance support for requirements-to-evidence substrate design	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 900.
[of the Director of National Intelligence, 2017a]	Intelligence Community Directive 121: Managing the Intelligence Community Information Environment	ic_information_environment_risk	information environment support for modular discovery, retrieval, and safeguarding claims	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 121.
[of the Director of National Intelligence, 2022]	Intelligence Community Directive 211: IC Support to the CFIUS Threat Analysis Process	economic_security_review	economic-security and due-diligence governance support for threat-analysis framing	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 211.
[of the Director of National Intelligence, 2013d]	Intelligence Community Directive 731: Supply Chain Risk Management	supply_chain_risk_governance	supply-chain risk governance support for defensive procurement and assurance lessons	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 731.
[of the Director of National Intelligence, 2013c]	Intelligence Community Directive 710: Classification and Control Markings System	classification_marking_governance	classification-marking context for caveat and dissemination-boundary lessons	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 710.
[of the Director of National Intelligence, 2013e]	Intelligence Community Directive 750: Counterintelligence Programs	counterintelligence_program_governance	counterintelligence program governance support for source-integrity and defensive awareness	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 750.
[Intelligence.gov, 2026e]	Mission	ic_public_transparency	public mission and values context for reader-facing IC orientation	Direct URL verified on 2026-06-14 through browser fetch because intelligence.gov returned 403 to plain curl; fetched HTML title and page content matched the mission page.
[Intelligence.gov, 2026b]	Our Values: Accountability	ic_public_transparency	public accountability and oversight context for legal/ethical framing	Direct URL verified on 2026-06-14 through browser fetch because intelligence.gov returned 403 to plain curl; fetched HTML title and page content matched the accountability page.
[Intelligence.gov, 2026f]	Our Values: Transparency	ic_public_transparency	public transparency context for release, public understanding, and source-protection boundaries	Direct URL verified on 2026-06-14 through browser fetch because intelligence.gov returned 403 to plain curl; fetched HTML title and page content matched the transparency page.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[Intelligence.gov, 2026a]	About This Site	ic_public_transparency	public transparency-platform context for orientation and publication-readiness posture	Direct URL verified on 2026-06-14 through browser fetch because intelligence.gov returned 403 to plain curl; fetched HTML title and page content matched the About This Site page.
[Intelligence.gov, 2026c]	Our Values: Collaboration	ic_public_transparency	public collaboration context for modular handoff, partner engagement, and source-pack routing	Direct URL verified on 2026-06-14 through browser fetch because intelligence.gov returned 403 to plain curl; fetched HTML title and page content matched the collaboration page.
[Intelligence.gov, 2026d]	Our Values: Innovation	ic_public_transparency	public innovation context for bounded agentic assistance and technology-governance framing	Direct URL verified on 2026-06-14 through browser fetch because intelligence.gov returned 403 to plain curl; fetched HTML title and page content matched the innovation page.
[Agency, 2024b]	Defense OSINT Strategy 2024-2028	defense_osint_governance	public OSINT governance and professionalization support, not collection procedure or live targeting guidance	Direct URL verified on 2026-06-14 through browser fetch because dia.mil returned 403 to plain curl; fetched PDF content matched the Defense OSINT Strategy.
[Agency, 2015]	DIA Style Manual for Intelligence Production	intelligence_writing_and_review	intelligence-production writing and style support for manuscript clarity and table/heading discipline	Direct URL verified on 2026-06-14 through browser fetch because dia.mil returned 403 to plain curl; fetched PDF metadata matched the DIA Style Manual.
[Agency, 2014]	DIA Instruction 5400.001: Privacy and Civil Liberties Program	rights_impact_privacy	privacy and civil-liberties governance support for legal/ethical review modules	Direct URL verified on 2026-06-14 through browser fetch because dia.mil returned 403 to plain curl; fetched PDF content matched DIAI 5400.001.
[Agency, 2026f]	NSA Cybersecurity Advisories and Guidance	cyber_defense_guidance_index	defensive cyber guidance index support for source routing and refresh duties	Direct URL verified on 2026-06-14 through browser fetch because nsa.gov returned 403 to plain curl; fetched HTML title and content matched the advisories and guidance page.
[Agency, 2026d]	About NSA Mission	ic_public_transparency	public mission context for SIGINT/cybersecurity orientation	Direct URL verified on 2026-06-14 through browser fetch because nsa.gov returned 403 to plain curl; fetched HTML title and content matched the NSA mission page.
[Agency, 2026e]	NSA Joins the ASD's ACSC and Others to Release Guidance on Agentic Artificial Intelligence Systems	agentic_ai_security_governance	agentic AI adoption and security-governance context, not an AGEINT benchmark	Direct URL verified on 2026-06-14 through browser fetch because nsa.gov returned 403 to plain curl; fetched HTML title and content matched the agentic AI services release.
[Agency, 2017b]	GEOINT Basic Doctrine Publication 1	geoint_professional_doctrine	GEOINT doctrine and geospatial-intelligence framing support	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from nga.mil.
[Agency, 2021]	NGA Releases New Data Strategy to Navigate Digital, GEOINT Revolution	geoint_data_governance	GEOINT data-governance and digital-transformation context for modular source substrate claims	Direct URL verified on 2026-06-14 with curl HTTP 200 and text/html content from nga.mil.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[of Investigation, 2026]	Counterintelligence and Espionage	counterintelligence_program_governance	Defines counterintelligence mission and defensive source-integrity context	Direct URL verified on 2026-06-14 through browser search/open because fbi.gov returned 403 to plain curl; fetched content matched the Counterintelligence and Espionage page.
[Office, 2026b]	About NRO History	declassified_reconnaissance_history	Declassified reconnaissance history support for historical and GEOINT source-provenance lessons	Direct URL verified on 2026-06-14 through web search/open; official NRO page content matched the history and Center for the Study of National Reconnaissance description.
[Dylan and Stivang, 2025]	Emerging Technologies and National Security Intelligence	ai_enabled_analysis_boundary	Supports bounded discussion of how AI, quantum technologies, and data-generating systems may reshape intelligence work; does not prove deployed AGEINT capability or abrupt transformation.	Direct Taylor and Francis source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[Caballero and Jenkins, 2024]	On Large Language Models in National Security Applications	ai_enabled_analysis_boundary	Supports bounded discussion of LLM assistance, hallucination, privacy, adversarial vulnerability, and supporting-role limits in national-security applications; not evidence for autonomous strategic judgment.	Direct arXiv source URL verified on 2026-06-15 with title, authors, abstract, DOI record, and subject metadata visible on the primary page.
[Mikhailov, 2023]	Optimizing National Security Strategies through LLM-Driven Artificial Intelligence Integration	ai_enabled_analysis_boundary	Provides discovery-grounded context for LLM-driven national-security strategy claims while requiring AGEINT prose to keep strategic claims bounded and evidence-bounded.	Direct arXiv source URL verified on 2026-06-15 with title, author, abstract, DOI metadata, and version history visible on the primary page.
[Revanth Gangi Reddy and Ji, 2023]	SmartBook: AI-Assisted Situation Report Generation for Intelligence Analysts	ai_enabled_analysis_boundary	Supports bounded discussion of AI-assisted situation-report generation and grounded summaries; reported study results are treated as source-specific, not AGEINT performance evidence.	Direct arXiv source URL verified on 2026-06-15 with title, authors, abstract, version metadata, and DOI record visible on the primary page.
[et al., 2024a]	Mind the Gap: Foundation Models and the Covert Proliferation of Military Intelligence, Surveillance, Target Acquisition, and Reconnaissance	ai_enabled_analysis_boundary	Supports bounded discussion of foundation-model risks for military intelligence, surveillance, target acquisition, and reconnaissance; AGEINT uses it for risk framing, not for operational ISTAR guidance.	Direct arXiv HTML source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2023a]	The Age of Synthetic Realities: Challenges and Opportunities	synthetic_media_provenance	Supports bounded discussion of synthetic realities, generated media, and provenance risk; does not support identity-attack recipes or unrestricted deepfake detection claims.	Direct arXiv source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2018]	The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation	ai_red_team_assurance	Supports high-level AI misuse taxonomy and defensive risk analysis only; AGEINT excludes operational instructions, target selection, evasion, and exploit procedures.	Direct arXiv source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[for Security and Technology, 2022]	Adversarial Machine Learning and Cybersecurity	ai_red_team_assurance	Supports defensive framing for adversarial machine learning and cybersecurity governance; does not provide exploit, evasion, or bypass instructions.	Direct CSET source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[Taddeo and Floridi, 2018]	Regulate Artificial Intelligence to Avert Cyber Arms Race	cyber_threat_intelligence	Supports bounded policy discussion of AI-enabled cyber escalation and arms-race risk; not technical guidance and not empirical AGEINT validation.	Direct Nature article page was opened and verified on 2026-06-15 after the script fetch timed out; title, authors, date, and DOI were visible on the primary page.
[Project and Institute, 2024]	The Future of Intelligence Analysis: U.S.-Australia Project on AI and Human-Machine Teaming	ai_enabled_analysis_boundary	Supports bounded discussion of AI human-machine teaming for all-source analysis; forward-looking recommendations remain policy context, not AGEINT performance evidence.	Direct SCSP report PDF was verified on 2026-06-15 through the current SCSP resource page after the attachment URL had moved.
[McMahon, 2024]	Analytic Tradecraft Standards in an Age of AI	analytic_tradecraft_evidence	Supports bounded discussion of analytic tradecraft standards under AI assistance; does not represent official U.S. government policy or validate AGEINT performance.	Direct Belfer report page and linked PDF were verified on 2026-06-15 after the attachment URL had moved; title, author, publication date, and report scope were visible.
[et al., 2019]	Analysis of Competing Hypotheses in Intelligence Analysis	sat_evaluation_evidence	Supports bounded scholarly discussion of ACH in intelligence analysis; does not imply ACH universally eliminates bias or guarantees analytic accuracy.	Direct Wiley source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2024b]	Task Structure, Confirmation Bias, and the Generation of Alternative Hypotheses	sat_evaluation_evidence	Supports bounded discussion of task structure and confirmation bias in hypothesis generation; not a universal debiasing or intelligence-success claim.	Direct SpringerOpen source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[The White House, 1988]	National Operations Security Program, NSDD 298	opsec_doctrine_governance	Provides official historical OPSEC policy context for critical-information protection and public doctrine framing; not an operational OPSEC playbook.	Direct Reagan Library PDF source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[Wardle and Derakhshan, 2017]	Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making	cognitive_influence_security	Supports taxonomy and terminology for information disorder, misinformation, disinformation, and malinformation; does not authorize manipulation or counter-propaganda practice.	Direct Council of Europe source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[Deng and UNIDIR, 2023]	Exploring Synthetic Data for Artificial Intelligence and Autonomous Systems: A Primer	model_data_provenance	Supports bounded discussion of synthetic data for AI and autonomous systems in international security, including benefits and limitations; not evidence for operational deployment readiness.	Direct UNIDIR report page and PDF were verified on 2026-06-15 after the attachment URL had moved; title, author, citation, and scope were visible.
[for Strategic and Studies, 2022]	Crossing the Deepfake Rubicon	synthetic_media_provenance	Supports bounded policy discussion of deepfake risk and governance; does not provide impersonation, targeting, or manipulation instructions.	Direct CSIS source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[National Security Agency et al., 2023]	Contextualizing Deepfake Threats to Organizations	synthetic_media_provenance	Supports defensive awareness and contextualization of deepfake threats; excludes impersonation guidance, targeting, evasion, and manipulation playbooks.	Direct defense.gov PDF source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[Agency, 2017a]	Active Social Engineering Defense	cyber_threat_intelligence	Supports public program-level framing for active social engineering defense; AGEINT uses it for defensive concept boundaries, not for social-engineering operations.	Direct DARPA source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2015]	Active Inference and Epistemic Value	cognitive_active_inference	Supports formal active-inference theory discussion around epistemic value and policy selection; does not validate AGEINT product performance or autonomous intent detection.	Direct PubMed source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2017]	Uncertainty, Epistemics and Active Inference	cognitive_active_inference	Supports scholarly discussion of uncertainty, epistemics, and active inference; not proof that AGEINT agents possess cognition or operational competence.	Direct PMC source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2022]	A Step-by-Step Tutorial on Active Inference and Its Application to Empirical Data	cognitive_active_inference	Supports step-by-step active-inference pedagogy and empirical-data modeling caveats; does not transfer automatically to intelligence-agent performance claims.	Direct PMC source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2021a]	Active Inference in Modeling Conflict	cognitive_active_inference	Supports bounded discussion of active-inference modeling in conflict scenarios; AGEINT treats it as theory/simulation context, not operational prediction or targeting evidence.	DOI redirected to the Zenodo primary record with HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[Kozera, 2020]	Fitness OSINT: Identifying and Tracking Military and Security Personnel with Fitness Applications	osint_geoint	Supports defensive discussion of fitness-app OSINT leakage and privacy risk; does not authorize tracking, doxxing, or targeting of real personnel.	Direct journal source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2025b]	Adversarial Machine Learning in Cybersecurity: A Review	ai_red_team_assurance	Supports defensive literature-review discussion of adversarial machine learning in cybersecurity; excludes exploit, evasion, and bypass procedures.	Direct journal source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2023b]	Challenges of Artificial Intelligence to Cognitive Security and Safety	cognitive_influence_security	Supports high-level scholarly discussion of AI challenges to cognitive security and safety; does not establish universal cognitive-security efficacy or manipulation countermeasures.	Direct journal PDF URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[Deppe and Schaal, 2024]	A Conceptual Framework and Method for a NATO ACT Concept for Cognitive Warfare	cognitive_influence_security	Supports bounded discussion of NATO cognitive-warfare concept development and terminology; not operational doctrine and not evidence for intervention efficacy.	Direct PMC source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[Terp and Breuer, 2022]	DISARM: A Framework for Analysis of Disinformation Campaigns	cognitive_influence_security	Supports defensive taxonomy and incident-analysis framing for influence operations; excludes persuasion campaign design, targeting, and manipulation guidance.	Direct IEEE source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2024c]	Large Language Models and Disinformation: A Double-Edged Sword	cognitive_influence_security	Supports bounded discussion of LLMs as both disinformation risks and defensive tools; does not authorize generation of deceptive content or manipulation campaigns.	Direct IEEE source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2025c]	Large Language Models Can Generate Election Disinformation	cognitive_influence_security	Supports bounded empirical discussion of LLM-generated election disinformation risk; AGEINT uses it for detection and governance caveats, not for content generation.	Direct PMC source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2023c]	Fighting Fire with Fire: Using Large Language Models to Combat Disinformation	cognitive_influence_security	Supports bounded discussion of using LLMs for defensive disinformation detection; does not establish universal detection reliability or endorse automated moderation.	Direct ACL Anthology PDF URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[Farid and Bohacek, 2022]	Protecting World Leaders Against Deep Fakes	synthetic_media_provenance	Supports bounded discussion of protecting public figures against deepfakes and synthetic impersonation; excludes identity-attack methods and targeting guidance.	Direct PMC source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2020]	Human Cognition Through the Lens of Social Engineering Cyberattacks	cognitive_influence_security	Supports defensive cognitive framing of social-engineering cyberattacks; excludes persuasion scripts, pretexting recipes, credential harvesting, and live targeting.	Direct PMC source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2021b]	Situation Awareness in Intelligence Scenarios	analytic_cognition_and_bias	Supports bounded discussion of situation awareness in intelligence scenarios; does not prove AGEINT learning outcomes or operational analyst performance.	Direct PMC source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2024d]	AI Emergency Preparedness	agent_incident_response	Supports bounded discussion of emergency preparedness for AI incidents; treated as preprint context for readiness planning, not settled policy or AGEINT incident-response evidence.	Direct arXiv source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2025a]	The AI Incident Regime	agent_incident_response	Supports bounded scholarly discussion of AI incident regimes and reporting design; does not replace official incident-reporting standards already encoded in AGEINT.	Direct arXiv HTML source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[Cooper, 2005]	Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis	analytic_tradecraft_evidence	Supports bounded claims about analytic-culture reform, self-correction, peer challenge, and limits of linear intelligence-cycle metaphors.	Direct CIA CSI book page verified live 2026-06-15; used for analytic-culture reform context, not as proof that any specific SAT improves accuracy.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[Janis, 1982]	Groupthink: Psychological Studies of Policy Decisions and Fiascoes	analytic_cognition_and_bias	Supports bounded classic groupthink and dissent-context framing, not a validated claim that one checklist eliminates group decision failure.	Google Books bibliographic record verified live 2026-06-15 for title, author, edition, publisher, year, and ISBN metadata; used as bibliographic support because no current publisher landing page was available.
[Coulthart, 2016]	Why Do Analysts Use Structured Analytic Techniques? An In-depth Study of an American Intelligence Agency	sat_evaluation_evidence	Supports bounded claims about SAT adoption motives and organizational use, not empirical proof that SATs improve accuracy across tasks.	Crossref DOI metadata verified live 2026-06-15 for title, author, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.
[Coulthart, 2017]	An Evidence-Based Evaluation of 12 Core Structured Analytic Techniques	sat_evaluation_evidence	Supports bounded technique-specific evidence-boundary claims about SATs and discourages treating the category as uniformly validated.	Crossref DOI metadata verified live 2026-06-15 for title, author, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.
[Tetlock, 2018]	Restructuring Structured Analytic Techniques in Intelligence	sat_evaluation_evidence	Supports bounded claims that SAT pedagogy should externalize reasoning, specify mechanisms, and avoid unsupported broad debiasing claims.	Crossref DOI metadata verified live 2026-06-15 for title, authors, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.
[Whitesmith, 2019]	The Efficacy of ACH in Mitigating Serial Position Effects and Confirmation Bias in an Intelligence Analysis Scenario	sat_evaluation_evidence	Supports bounded claims about ACH evidence for bias mitigation under a specific intelligence-analysis scenario.	Crossref DOI metadata verified live 2026-06-15 for title, author, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.
[Mandel, 2020]	Coherence of Probability Judgments from Uncertain Evidence: Does ACH Help?	sat_evaluation_evidence	Supports bounded claims that ACH should be treated as a diagnostic aid whose probabilistic coherence gains are disputed and task-dependent.	Cambridge Core article page verified live 2026-06-15 for title, authors, journal record, and accessible article metadata.
[Dhami, 2018]	Boosting Intelligence Analysts' Judgment Accuracy: What Works, What Fails?	forecasting_calibration_evidence	Supports bounded claims that calibration, coherentization, and aggregation can complement SATs without making ACH a universal accuracy intervention.	Cambridge Core article page verified live 2026-06-15 for title, authors, journal record, and accessible article metadata.
[Tetlock, 2015b]	Improving Intelligence Analysis With Decision Science	forecasting_calibration_evidence	Supports bounded claims that decision-science tools such as calibration, aggregation, and uncertainty communication complement SAT practice.	Crossref DOI metadata verified live 2026-06-15 for title, authors, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.
[Council, 2011]	Intelligence Analysis for Tomorrow: Advances from the Behavioral and Social Sciences	analytic_cognition_and_bias	Supports bounded claims about using behavioral and social science to improve analysis, training, and evaluation without claiming technique-level guarantees.	National Academies publisher record verified live 2026-06-15; Crossref DOI metadata for 10.17226/13040 verified title, publisher, and year.
[on Intelligence, 2004]	Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq	intelligence_failure_postmortem	Supports bounded postmortem claims about Iraq WMD assessment failures and the need for explicit assumptions, source quality, dissent, and caveats.	Official Senate Intelligence Committee PDF URL verified live 2026-06-15 with successful redirect to current Senate-hosted PDF asset.
[Activity, 2010]	Aggregative Contingent Estimation	forecasting_calibration_evidence	Supports bounded claims about government-sponsored probabilistic forecasting, elicitation, weighting, aggregation, and empirical testing against real events.	Direct IARPA program page verified live 2026-06-15; used for program objectives and forecasting-evidence context, not as an AGEINT performance claim.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[Activity, 2023]	Rapid Explanation, Analysis and Sourcing Online	agentic_analytic_assistance	Supports bounded claims that AI-enabled reasoning systems can assist evidence discovery and reasoning review while retaining analyst responsibility.	Direct IARPA program page verified live 2026-06-15; used for bounded analyst-assistance context and explicit non-replacement language.
[Helmer, 1963]	An Experimental Application of the DELPHI Method to the Use of Experts	forecasting_calibration_evidence	Supports bounded claims about Delphi as an expert-elicitation and judgment-aggregation technique, not proof that expert panels converge on truth.	Crossref DOI metadata verified live 2026-06-15 for title, authors, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.
[Klein, 2007]	Performing a Project Premortem	analytic_method_pedagogy	Supports bounded classroom use of premortem thinking as a failure-imagination aid, not a validated guarantee of risk detection.	Harvard Business Review article page verified live 2026-06-15 for title, author, publication date, and publisher record.
[Marrin, 2012]	Improving Intelligence Analysis: Bridging the Gap between Scholarship and Practice	analytic_method_pedagogy	Supports bounded claims about bridging intelligence scholarship, analytic practice, and training without treating scholarship uptake as a finished solution.	Crossref DOI metadata verified live 2026-06-15 for title, author, publisher, and year; DOI URL retained as stable scholarly source.
[Svenmarck, 2021]	Overview of Structured Analytic Techniques for Assessment and Judgement of Major Events	analytic_method_pedagogy	Supports bounded claims that SAT catalogues are used in public-sector training contexts and classify techniques by purpose and facilitation needs.	FOI report-summary page verified live 2026-06-15 for title, author, report number FOI-R–5116–SE, date, abstract, and keywords.
[Service, 2021]	Technical Brief on Joint Structured Analysis Techniques	analytic_method_pedagogy	Supports bounded claims about collaborative SAT facilitation, dissent, uncertainty management, and technique selection in humanitarian analysis contexts.	JIPS publication page verified live 2026-06-15 for title, authoring organization, date, purpose statement, and download link.
[Denzler, 2024]	Revisiting the Psychology of Structured Analytical Techniques	analytic_cognition_and_bias	Supports bounded claims about SAT psychology and cognitive assumptions without treating technique use as validated bias elimination.	Crossref DOI metadata verified live 2026-06-15 for title, author, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.
[Mandel, 2024]	Critical Review of the Analysis of Competing Hypotheses Technique: Lessons for the Intelligence Community	sat_evaluation_evidence	Supports bounded ACH caveats and lessons for intelligence practice, not claims that AGEINT validates ACH replacement or automation.	Crossref DOI metadata verified live 2026-06-15 for title, authors, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.
[Miksa, 2024]	Assessment Tabling: An Integrated Structured Analytic Technique for Improved Intelligence Analysis and Reasoning Visualisation	analytic_method_pedagogy	Supports bounded claims about reasoning visualization as an analytic artifact design pattern, not empirical proof of accuracy improvement.	Crossref DOI metadata verified live 2026-06-15 for title, author, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.
[Coulthart, 2025]	Structured Analytic Techniques in an Intelligence Fusion Centre: A Survey of Analyst Perspectives and Use	sat_evaluation_evidence	Supports bounded claims about SAT use and perceptions in fusion-centre practice, not direct proof of analytic accuracy gains.	Crossref DOI metadata verified live 2026-06-15 for title, authors, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.
[Gustafson, 2025]	Teaching Structured Analytic Techniques across Nations: Same, Same but Different	analytic_method_pedagogy	Supports bounded claims about SAT teaching across institutional and national contexts without assuming one curriculum design transfers unchanged.	Crossref DOI metadata verified live 2026-06-15 for title, authors, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.
[McCarthy, 2024]	Seeing the Futures: Evaluating the Application of Structured Analytic Technique Alternative Futures Analysis	warning_intelligence	Supports bounded claims about Alternative Futures Analysis as a scenario and indicator aid whose value depends on purpose-fit and application context.	National Security Journal article page verified live 2026-06-15 for title, author, publication date, DOI, abstract, and PDF link.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[Ritchey, 2013]	General Morphological Analysis: A General Method for Non-Quantified Modelling	analytic_method_pedagogy	Supports bounded claims about morphological analysis as a structuring method for non-quantified multidimensional problems, not as analytic validation by itself.	Swedish Morphological Society method page verified live 2026-06-15 for title, author, revision note, and method description; used as a public method source for Zwicky-derived morphological analysis.
[Pherson, 2014b]	Cases in Intelligence Analysis: Structured Analytic Techniques in Action	analytic_method_pedagogy	Supports bounded claims about SAT case pedagogy, technique templates, and classroom application rather than empirical technique efficacy.	SAGE College Publishing product page verified live 2026-06-15 for title, subtitle, authors, edition, publisher, date, ISBNs, and description.
[Pherson, 2020]	Critical Thinking for Strategic Intelligence	analytic_method_pedagogy	Supports bounded claims about critical-thinking pedagogy, source evaluation, uncertainty communication, and analytic graphics rather than automated judgment replacement.	SAGE College Publishing product page verified live 2026-06-15 for title, authors, third edition, publisher, date, ISBNs, and description.
[of the Army., 2006]	FM 2-22.3 Human Intelligence Collector Operations	humint_doctrine	Supports bounded AGEINT discussion of humint_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_army_fm_2_22_3_humint retained.
[of the Director of National Intelligence., 2008]	ICD 304: Human Intelligence	humint_doctrine	Supports bounded AGEINT discussion of humint_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_odni_icd_304_humint retained.
[of the Director of National Intelligence., 2016]	ICD 310: Coordination of Clandestine Human Source Collection Outside the US	humint_doctrine	Supports bounded AGEINT discussion of humint_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_odni_icd_310_clandestine_hum retained.
[to Study Governmental Operations with Respect to Intelligence Activities, Church Committeea]	Church Committee Final Report Book I: Foreign and Military Intelligence (S. Rep. 94-755)	humint_oversight_history	Supports bounded AGEINT discussion of humint_oversight_history and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key public_church_committee_book_i_197 retained.
[to Study Governmental Operations with Respect to Intelligence Activities, Church Committeeb]	Church Committee Book III: NSA Surveillance (S. Rep. 94-755)	sigint_oversight_history	Supports bounded AGEINT discussion of sigint_oversight_history and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key public_church_committee_book_iii_nsa retained.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[of the Director of National Intelligence., 2007]	ICD 302: Document and Media Exploitation	humint_doctrine	Supports bounded AGEINT discussion of humint_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_odni_icd_302_domex retained.
[of the Joint Chiefs of Staff., 2012]	JP 2-01: Joint and National Intelligence Support to Military Operations (2012)	collection_management_doctrine	Supports bounded AGEINT discussion of collection_management_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_jp_2_01_intelligence_support_ retained.
[Agency., n.d.]	TEMPEST: A Signal Problem (NSA Declassified)	sigint_emanations_intelligence	Supports bounded AGEINT discussion of sigint_emanations_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_nsa_tempest_signal_problem retained.
[National Security Agency, Various years]	NSA Center for Cryptologic History: Historical Publications	sigint_history	Supports bounded AGEINT discussion of sigint_history and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_nsa_center_cryptologic_history retained.
[of Standards and Technology., 2024a]	FIPS 203: ML-KEM Post-Quantum Key-Encapsulation Standard	cryptography_standards	Supports bounded AGEINT discussion of cryptography_standards and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_nist_fips_203_ml_kem retained.
[of Standards and Technology., 2024b]	FIPS 204: ML-DSA Post-Quantum Digital Signature Standard	cryptography_standards	Supports bounded AGEINT discussion of cryptography_standards and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_nist_fips_204_ml_dsa retained.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[of Standards and Technology., 2024c]	FIPS 205: SLH-DSA Post-Quantum Hash-Based Signature Standard	cryptography_standards	Supports bounded AGEINT discussion of cryptography_standards and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_nist_fips_205_slh_dsa retained.
[Office of the Director of National Intelligence, 2022]	ODNI Declassified Report on Commercially Available Information (2022)	osint_doctrine	Supports bounded AGEINT discussion of osint_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_odni_cai_report_2022 retained.
[of the Joint Chiefs of Staff., 2017]	JP 2-03: Geospatial Intelligence in Joint Operations (2017)	geoint_doctrine	Supports bounded AGEINT discussion of geoint_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_jp_2_03_geoint_joint_ops_20 retained.
[Clark, 2020]	Geospatial Intelligence: Origins and Evolution (Georgetown UP, 2020)	geoint_tradecraft	Supports bounded AGEINT discussion of geoint_tradecraft and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_clark_2020_geospatial_intellig retained; stale or indirect proposal URL replaced with direct source record.
[Van Puyvelde, 2025]	The rise of open-source intelligence, EJIS 2025	osint_methodology	Supports bounded AGEINT discussion of osint_methodology and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_van_puyvelde_2025_rise_osint retained.
[of the Director of National Intelligence., Current]	ICD 206: Sourcing Requirements for Disseminated Analytic Products (with ICS 206-01 on PAI/CAI/OSINT)	osint_doctrine	Supports bounded AGEINT discussion of osint_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_odni_icd_206_sourcing_osint_ retained.
[Agency., 2018]	NGA Pub 1.0: GEOINT Basic Doctrine (2018)	geoint_doctrine	Supports bounded AGEINT discussion of geoint_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_nga_geoint_pub1_doctrine_20 retained.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[of the Director of National Intelligence., 2024]	ODNI Commercially Available Information Fact Sheet (May 2024)	osint_doctrine	Supports bounded AGEINT discussion of osint_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_odni_cai_fact_sheet_2024 retained.
[Hutchins, 2011]	Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains	cyber_threat_intelligence	Supports bounded AGEINT discussion of cyber_threat_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_hutchins_2011_kill_chain normalized to professional_hutchins_2011_kill_chain.
[Caltagirone, 2013]	The Diamond Model of Intrusion Analysis	cyber_threat_intelligence	Supports bounded AGEINT discussion of cyber_threat_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_caltagirone_2013_diamond_mo normalized to professional_caltagirone_2013_diamond_
[CISA, 2024]	PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure (AA24-038A)	apt_threat_intelligence	Supports bounded AGEINT discussion of apt_threat_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_cisa_aa24_038a_volt_typhoon retained.
[NSA, 2023]	PRC State-Sponsored Cyber Actor Living off the Land to Evade Detection (AA23-144A)	apt_threat_intelligence	Supports bounded AGEINT discussion of apt_threat_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_cisa_aa23_144a_volt_typhoon_ retained.
[DOE, 2022]	APT Cyber Tools Targeting ICS/SCADA Devices (AA22-103A)	apt_threat_intelligence	Supports bounded AGEINT discussion of apt_threat_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_cisa_aa22_103a_apt_ics_scada retained.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[CISA., 2020]	Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations (AA20-352A)	supply_chain_intelligence_attacks	Supports bounded AGEINT discussion of supply_chain_intelligence_attacks and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_cisa_aa20_352a_solarwinds retained.
[Lee, 2016]	Analysis of the Cyber Attack on the Ukrainian Power Grid	historical_ics_incidents	Supports bounded AGEINT discussion of historical_ics_incidents and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_eisac_sans_ukraine_2016 retained.
[for Cybersecurity, ENISA]	ENISA Threat Landscape 2024	cyber_threat_intelligence	Supports bounded AGEINT discussion of cyber_threat_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_enisa_threat_landscape_2024 retained.
[Boyens, 2022]	Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (NIST SP 800-161 Rev. 1)	supply_chain_intelligence_attacks	Supports bounded AGEINT discussion of supply_chain_intelligence_attacks and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_nist_sp_800_161r1_scrm retained.
[Biden, 2021]	Executive Order 14028 on Improving the Nation's Cybersecurity	supply_chain_intelligence_attacks	Supports bounded AGEINT discussion of supply_chain_intelligence_attacks and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_whitehouse_eo_14028 retained; stale or indirect proposal URL replaced with direct source record.
[of Incident Response and Teams, FIRST]	Traffic Light Protocol (TLP) — FIRST Standards Definitions and Usage Guidance, Version 2.0	threat_intel_sharing_standards	Supports bounded AGEINT discussion of threat_intel_sharing_standards and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_first_tlp_v2 retained.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[Corporation, NERC]	NERC CIP Reliability Standards (CIP-002 through CIP-015)	ics_ot_security_standards	Supports bounded AGEINT discussion of ics_ot_security_standards and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_nerc_cip_standards retained.
[Cherepanov, 2017]	Win32/Industroyer: A New Threat for Industrial Control Systems	historical_ics_incidents	Supports bounded AGEINT discussion of historical_ics_incidents and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_eset_win32_industroyer_2017 normalized to professional_eset_win32_industroyer_201
[ICS-CERT., 2010]	ICSA-10-272-01: Stuxnet Malware Mitigation	historical_ics_incidents	Supports bounded AGEINT discussion of historical_ics_incidents and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_cisa_isc_cert_stuxnet_advisory retained.
[CISA., 2022]	Control System Defense: Know the Opponent	ics_ot_security_standards	Supports bounded AGEINT discussion of ics_ot_security_standards and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_cisa_nsa_ics_know_opponent_ retained.
[ICS., 2017]	ICS Defense Use Case No. 6: Modular ICS Malware	historical_ics_incidents	Supports bounded AGEINT discussion of historical_ics_incidents and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_nerc_eisac_ukraine_duc6_2017 retained.
[for Network and Security, ENISA]	Protecting Industrial Control Systems: Recommendations for Europe and Member States	ics_ot_security_standards	Supports bounded AGEINT discussion of ics_ot_security_standards and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_enisa_protecting_ics_2011 retained; stale or indirect proposal URL replaced with direct source record.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[of Staff., 2012]	JP 3-13, Information Operations (2012)	information_operations_doctrine	Supports bounded AGEINT discussion of information_operations_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_dod_jp3_13_information_oper retained.
[of Staff., 2014b]	JP 3-13.2, Military Information Support Operations (2014)	psyop_miso_doctrine	Supports bounded AGEINT discussion of psyop_miso_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_dod_jp3_13_2_miso retained.
[Paul and Matthews., 2016]	The Russian "Firehose of Falsehood" Propaganda Model (RAND, 2016)	active_measures_disinformation	Supports bounded AGEINT discussion of active_measures_disinformation and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_rand_paul_matthews_firehose_ normalized to professional_rand_paul_matthews_firehos
[Lazer, 2018]	The science of fake news (Science, 2018)	disinformation_misinformation_science	Supports bounded AGEINT discussion of disinformation_misinformation_science and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_lazer_2018_science_fake_news retained.
[Network, FinCEN]	FinCEN SAR Narrative Guidance Package (2003/2006)	finint_sar_reporting	Supports bounded AGEINT discussion of finint_sar_reporting and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_fincen_sar_narrative_guidance retained.
[of Financial Intelligence Units., 2023]	Egmont Group Principles for Information Exchange Between FIUs (April 2023)	finint_international_cooperation	Supports bounded AGEINT discussion of finint_international_cooperation and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_egmont_group_fiu_principles retained.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[on Drugs and Crime, UNODC]	UNODC Money Laundering, Proceeds of Crime and the Financing of Terrorism	finint_aml_cft_international	Supports bounded AGEINT discussion of finint_aml_cft_international and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_unodc_money_laundering_over retained.
[Schott, 2006]	World Bank/IMF Reference Guide to AML/CFT (2006)	finint_aml_cft_international	Supports bounded AGEINT discussion of finint_aml_cft_international and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_worldbank_aml_reference_guid retained.
[Counterintelligence and Center, NCSCb]	National Counterintelligence Strategy 2024 (NCSC/ODNI)	counterintelligence_strategy	Supports bounded AGEINT discussion of counterintelligence_strategy and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_ncsc_national_ci_strategy_202 retained.
[Counterintelligence and Center, NCSCa]	National Counterintelligence Strategy 2020–2022 (NCSC/ODNI)	counterintelligence_strategy	Supports bounded AGEINT discussion of counterintelligence_strategy and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_ncsc_national_ci_strategy_202 retained.
[Pennycook and Rand., 2021]	The psychology of fake news (Trends in Cognitive Sciences, 2021)	disinformation_cognitive_psychology	Supports bounded AGEINT discussion of disinformation_cognitive_psychology and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_pennycook_rand_2021_psycho retained.
[Starbird and Wilson., 2019]	Disinformation as Collaborative Work (ACM CSCW, 2019)	active_measures_information_operations	Supports bounded AGEINT discussion of active_measures_information_operations and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_starbird_arif_wilson_2019_dis retained.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[Hoffman, 2007]	Conflict in the 21st Century: The Rise of Hybrid Wars (Potomac Institute, 2007)	hybrid_warfare_doctrine	Supports bounded AGEINT discussion of hybrid_warfare_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_hoffman_2007_hybrid_wars retained.
[Mazarr, 2015]	Mastering the Gray Zone (USAWC Press, 2015)	gray_zone_competition_doctrine	Supports bounded AGEINT discussion of gray_zone_competition_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_mazarr_2015_gray_zone retained.
[of Defense., 2020]	Irregular Warfare Annex to the National Defense Strategy – Summary (DoD, 2020)	irregular_warfare_strategy	Supports bounded AGEINT discussion of irregular_warfare_strategy and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_dod_iw_annex_2020 retained.
[of Staff., 2014a]	JP 3-05, Special Operations (2014)	special_operations_doctrine	Supports bounded AGEINT discussion of special_operations_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_dod_jp3_05_special_operation retained.
[Cialdini, 1984]	Influence: The Psychology of Persuasion (Cialdini, 1984)	social_engineering_influence_psychology	Supports bounded AGEINT discussion of social_engineering_influence_psychology and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_cialdini_1984_influence_psych retained; stale or indirect proposal URL replaced with direct source record.
[of Excellence., 2021]	NATO StratCom COE Strategic Communications Hybrid Threats Toolkit (2021)	hybrid_warfare_stratcom	Supports bounded AGEINT discussion of hybrid_warfare_stratcom and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_nato_stratcom_hybrid_threats retained.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[of Staff., 2013]	JP 2-0, Joint Intelligence (2013)	imint_joint_intelligence_doctrine	Supports bounded AGEINT discussion of imint_joint_intelligence_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_dod_jp2_0_joint_intelligence retained.
[Pamment and Smith., 2022]	Attributing Information Influence Operations (NATO StratCom COE, 2022)	active_measures_attribution	Supports bounded AGEINT discussion of active_measures_attribution and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_nato_stratcom_attributing_iio retained.
[Andrew, 1990]	KGB: The Inside Story	intelligence_history_soviet	Supports bounded AGEINT discussion of intelligence_history_soviet and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_andrew_gordievsky_1990_kgb retained.
[Andrew, 1999]	The Sword and the Shield	intelligence_history_soviet	Supports bounded AGEINT discussion of intelligence_history_soviet and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_andrew_mitrokhin_1999_sword retained.
[Andrew, 2009]	The Defence of the Realm	intelligence_history_british_allied	Supports bounded AGEINT discussion of intelligence_history_british_allied and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_andrew_2009_defend_realm retained.
[Weiner, 2007]	Legacy of Ashes: The History of the CIA	intelligence_history_american	Supports bounded AGEINT discussion of intelligence_history_american and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_weiner_2007_legacy_ashes retained; stale or indirect proposal URL replaced with direct source record.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[to Study Governmental Operations with Respect to Intelligence Activities., 1976]	Church Committee Final Report (Internet Archive)	legal_oversight_intelligence	Supports bounded AGEINT discussion of legal_oversight_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key public_church_committee_1976_final_r retained.
[Tversky, 1974]	Judgment under Uncertainty: Heuristics and Biases	cognitive_bias_foundations	Supports bounded AGEINT discussion of cognitive_bias_foundations and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_tversky_kahneman_1974_judg retained.
[Kahneman, 2011]	Thinking, Fast and Slow (Wikipedia)	cognitive_bias_foundations	Supports bounded AGEINT discussion of cognitive_bias_foundations and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_kahneman_2011_thinking_fast retained; stale or indirect proposal URL replaced with direct source record.
[Lewandowsky, 2021]	Countering Misinformation through Inoculation and Prebunking	cognitive_security_inoculation	Supports bounded AGEINT discussion of cognitive_security_inoculation and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_lewandowsky_vanderlinden_20 retained.
[Lewandowsky, 2020]	The Debunking Handbook 2020	cognitive_security_inoculation	Supports bounded AGEINT discussion of cognitive_security_inoculation and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_lewandowsky_cook_2020_debu retained.
[Pennycook, 2021]	Shifting Attention to Accuracy — Nature	cognitive_security_misinformation	Supports bounded AGEINT discussion of cognitive_security_misinformation and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_pennycook_2021_accuracy_nu retained.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[Tetlock, 2005]	Expert Political Judgment — Internet Archive	analytic_tradecraft_forecasting	Supports bounded AGEINT discussion of analytic_tradecraft_forecasting and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_tetlock_2005_expert_political_ retained.
[Tetlock, 2015a]	Superforecasting — Google Play Books	analytic_tradecraft_forecasting	Supports bounded AGEINT discussion of analytic_tradecraft_forecasting and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_tetlock_gardner_2015_superfo retained; stale or indirect proposal URL replaced with direct source record.
[Congress., 1978]	FISA 1978 — GovInfo (Statutes at Large)	legal_authorities_surveillance	Supports bounded AGEINT discussion of legal_authorities_surveillance and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_fisa_1978_statute retained.
[Congress., 2001]	USA PATRIOT Act — GovInfo Compilation	legal_authorities_surveillance	Supports bounded AGEINT discussion of legal_authorities_surveillance and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_usa_patriot_act_2001 retained.
[Congress., 2015]	USA FREEDOM Act — GovInfo	legal_authorities_surveillance	Supports bounded AGEINT discussion of legal_authorities_surveillance and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_usa_freedom_act_2015 retained.
[Reagan, 1981]	EO 12333 — ODNI	legal_authorities_intelligence_collection	Supports bounded AGEINT discussion of legal_authorities_intelligence_collection and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key official_eo_12333_odni_text retained; stale or indirect proposal URL replaced with direct source record.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[Quinlan, 2007]	Just Intelligence: Prolegomena — Semantic Scholar	ethics_of_intelligence	Supports bounded AGEINT discussion of ethics_of_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_quinlan_2007_just_intelligence retained.
[Omand, 2010]	Securing the State — Google Books	ethics_of_intelligence	Supports bounded AGEINT discussion of ethics_of_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_omand_2010_securing_the_sta retained.
[Omand, 2018]	Principled Spying — Georgetown University Press	ethics_of_intelligence	Supports bounded AGEINT discussion of ethics_of_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_omand_phythian_2018_princi retained.
[Russell, 2020]	Artificial Intelligence: A Modern Approach, 4th ed.	agent_foundations	Supports bounded AGEINT discussion of agent_foundations and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_russell_norvig_2020_aima retained.
[Rao, 1995]	BDI Agents: From Theory to Practice	agent_foundations	Supports bounded AGEINT discussion of agent_foundations and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_rao_georgeff_1995_bdi retained.
[Vaswani, 2017]	Attention Is All You Need	llm_architecture	Supports bounded AGEINT discussion of llm_architecture and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_vaswani_2017_attention retained.
[Yao, 2023b]	Tree of Thoughts: Deliberate Problem Solving with LLMs	agentic_reasoning	Supports bounded AGEINT discussion of agentic_reasoning and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_yao_2023_tree_of_thoughts retained.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[Lewis, 2020]	Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks	agentic_memory	Supports bounded AGEINT discussion of agentic_memory and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_lewis_2020_rag retained.
[Patil, 2023]	Gorilla: Large Language Model Connected with Massive APIs	tool_use_agents	Supports bounded AGEINT discussion of tool_use_agents and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_patil_2023_gorilla retained.
[Qin, 2023]	ToolLLM: Facilitating Large Language Models to Master 16000+ Real-world APIs	tool_use_agents	Supports bounded AGEINT discussion of tool_use_agents and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_qin_2023_toolllm retained.
[Wu, 2023]	AutoGen: Enabling Next-Gen LLM Applications via Multi-Agent Conversation	multi_agent_frameworks	Supports bounded AGEINT discussion of multi_agent_frameworks and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_wu_2023_autogen retained.
[LangChain, 2025a]	LangChain Documentation	agentic_framework_docs	Supports bounded AGEINT discussion of agentic_framework_docs and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key professional_langchain_documentation retained.
[LangChain, 2025b]	LangGraph Documentation	agentic_framework_docs	Supports bounded AGEINT discussion of agentic_framework_docs and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key professional_langgraph_documentation retained.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[CrewAI, 2025]	CrewAI Documentation	agentic_framework_docs	Supports bounded AGEINT discussion of agentic_framework_docs and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key profes-sional_crewai_documentation retained.
[Liang, 2022]	Holistic Evaluation of Language Models	llm_evaluation	Supports bounded AGEINT discussion of llm_evaluation and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key schol-arly_liang_2022_helm retained.
[Srivastava, 2022]	Beyond the Imitation Game: Quantifying and Extrapolating the Capabilities of LLMs	llm_evaluation	Supports bounded AGEINT discussion of llm_evaluation and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key schol-arly_srivastava_2022_bigbench retained.
[Perez, 2022]	Ignore Previous Prompt: Attack Techniques For Language Models	adversarial_ai_security	Supports bounded AGEINT discussion of adversarial_ai_security and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key schol-arly_perez_2022_prompt_injection retained.
[Ericsson, 1993]	The Role of Deliberate Practice in the Acquisition of Expert Performance	cognitive_performance	Supports bounded AGEINT discussion of cognitive_performance and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key schol-arly_ericsson_1993_deliberate_prac retained.
[Cepeda, 2006]	Distributed Practice in Verbal Recall Tasks	cognitive_performance	Supports bounded AGEINT discussion of cognitive_performance and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key schol-arly_cepeda_2006_spaced_repetitio retained.

Anchor	Source	Lane	Contribution to the manuscript	Verification caveat
[Walker, 2006]	Sleep, Memory, and Plasticity	cognitive_performance	Supports bounded AGEINT discussion of cognitive_performance and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_walker_stickgold_2006_sleep_ retained.
[Kaplan, 1989]	The Experience of Nature: A Psychological Perspective	cognitive_performance	Supports bounded AGEINT discussion of cognitive_performance and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_kaplan_kaplan_1989_attentior retained; stale or indirect proposal URL replaced with direct source record.
[of Standards and Technology., 2024]	NIST IR 8547: Transition to Post-Quantum Cryptography Standards	cryptographic_standards	Supports bounded AGEINT discussion of cryptographic_standards and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Draft status retained. Direct source URL reviewed on 2026-06-16; original proposal key official_nist_pqc_migration_ir8547 retained.
[Weng, 2023]	LLM-powered Autonomous Agents	agentic_design_principles	Supports bounded AGEINT discussion of agentic_design_principles and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_weng_2023_agent_survey normalized to professional_weng_2023_agent_survey.

80.3 Source refresh ledger: cadence, checked dates, and due-status evidence

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Agency, 2009]	A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis	analytic_tradecraft	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Agency, 2016]	A Tradecraft Primer: Basic Structured Analytic Techniques	analytic_tradecraft	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of the Director of National Intelligence, 2026d]	Intelligence Community Directive 206: Sourcing Requirements for Disseminated Analytic Products	analytic_tradecraft	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of the Director of National Intelligence, 2026e]	Objectivity and IC Analytic Standards	analytic_tradecraft	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of State, 2024]	Open Source Intelligence Strategy	osint_geoint	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Jr., 2007]	Psychology of Intelligence Analysis	analytic_tradecraft	scholarly_or_official	2026-06-06	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use; URL refreshed 2026-06-06 after liveness check.
[of the Director of National Intelligence, 2026c]	Intelligence Community Directive 204: National Intelligence Priorities Framework	collection_management	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[of Staff, 2026]	JP 2-0: Joint Intelligence	collection_management	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of the Army, 2020]	ATP 2-33.4: Intelligence Analysis	analytic_tradecraft	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Counterintelligence and Center, 2024]	The National Counterintelligence Strategy	counterintelligence_source_integrity	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of the Director of National Intelligence and Agency, 2024]	The INT of First Resort: The IC OSINT Strategy 2024-2026	osint_geoint	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Agency, 2026c]	NGA Strategy	osint_geoint	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Archives and Administration, 1981]	Executive Order 12333: United States Intelligence Activities	legal_oversight	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Agency, 2026g]	Foreign Intelligence Surveillance Act	legal_oversight	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Community, 2026]	How the IC Works	governed_intelligence_cycle	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Community, 2020b]	Principles of Artificial Intelligence Ethics for the Intelligence Community	ai_ethics_data_governance	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Community, 2020a]	Artificial Intelligence Ethics Framework for the Intelligence Community	ai_ethics_data_governance	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of the Director of National Intelligence, 2025b]	Intelligence Community Directive 505: Artificial Intelligence	ai_ethics_data_governance	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of the Director of National Intelligence, 2025a]	Intelligence Community Directive 504: Intelligence Community Data Management	ai_ethics_data_governance	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of the Director of National Intelligence, 2026b]	Authorized Classification and Control Markings Register	governed_intelligence_cycle	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Privacy and Board, 2026]	Oversight Reports	legal_oversight	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[General Services Administration et al., 2026]	Federal Data Strategy	ai_ethics_data_governance	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Agency, 2026a]	Center for the Study of Intelligence	historical_declassified_sources	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Agency, 2026h]	NSA Historical Releases	historical_declassified_sources	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Office, 2026a]	Declassified NRO Programs and Projects	historical_declassified_sources	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Archives and Administration, 2026b]	Records of the Central Intelligence Agency	historical_declassified_sources	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Network, 2026a]	FinCEN Alerts, Advisories, Notices, Bulletins, and Fact Sheets	financial_economic_security	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Foreign Assets Control, 2026]	Sanctions Programs and Country Information	financial_economic_security	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Force, 2025]	The FATF Recommendations	financial_economic_security	international_standard	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Industry and Security, 2026]	Export Enforcement	financial_economic_security	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Authority, 2026]	Model AI Governance Framework for Agentic AI	agentic_ai_governance	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[ASD ACSC and NCSC-UK, 2026]	Careful Adoption of Agentic AI Services	agentic_ai_governance	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Standards and Technology, 2026a]	Accelerating the Adoption of Software and Artificial Intelligence Agent Identity and Authorization	agentic_ai_governance	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Standards and Technology, 2026c]	AI Agent Standards Initiative	agent_interoperability	official_primary	2026-06-11	quarterly	NIST AI-agent standards initiative, RFI, guidance, technical convening, protocol, identity, or evaluation deliverable changes	Direct NIST source URL verified live 2026-06-11; page identifies the AI Agent Standards Initiative as focused on trusted, interoperable, and secure agentic AI.
[UK Department for Science et al., 2024]	AI Safety Institute Approach to Evaluations	agentic_ai_governance	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Project, 2026b]	OWASP Top 10 for Agentic Applications for 2026	agentic_ai_security	security_standard	2026-06-11	semiannual	OWASP Agentic Applications Top 10 version, risk category, mitigation guidance, or project URL changes	Direct OWASP GenAI Security Project resource verified live 2026-06-11 with the 2026 Agentic Applications Top 10 scope and peer-reviewed security-risk framing.
[MITRE, 2026a]	MITRE ATLAS	ai_red_team_assurance	research_standard	2026-06-11	quarterly	MITRE ATLAS tactic, technique, mitigation, case-study, or matrix-version changes	Direct MITRE ATLAS source URL verified live 2026-06-11; page identifies ATLAS as a globally accessible living knowledge base of adversary tactics and techniques against AI systems.
[Project, 2025d]	OWASP Top 10 for Large Language Model Applications	agentic_ai_governance	security_standard	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Standards and Technology, 2022d]	Secure Software Development Framework, NIST SP 800-218	agentic_ai_governance	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Standards and Technology, 2024f]	The NIST Cybersecurity Framework (CSF) 2.0	ics_ot_defense	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Standards and Technology, 2022b]	Engineering Trustworthy Secure Systems, NIST SP 800-160 Vol. 1 Rev. 1	ics_ot_defense	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Standards and Technology, 2016]	Guide to Cyber Threat Information Sharing, NIST SP 800-150	cyber_threat_intelligence	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[of Standards and Technology, 2025c]	Incident Response Recommendations and Considerations, NIST SP 800-61 Rev. 3	cyber_threat_intelligence	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Standards and Technology, 2022c]	Cybersecurity Supply Chain Risk Management Practices, NIST SP 800-161 Rev. 1	cyber_threat_intelligence	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Cybersecurity and Agency, 2026c]	ICS Recommended Practices	ics_ot_defense	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Cybersecurity and Agency, 2026f]	CISA Tabletop Exercise Packages	ics_ot_defense	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Standards and Technology, 2006]	Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities	ics_ot_defense	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[MITRE, 2026c]	MITRE ATT&CK for ICS Matrix	ics_ot_defense	research_standard	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[for Security Policy, 2025]	Enhancing Cognitive Security and Societal Resilience to Counter Cognitive Warfare	cognitive_influence_security	scholarly_policy	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[NSA and partners, 2025]	Principles for the Secure Integration of Artificial Intelligence in Operational Technology	ics_ot_defense	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Foundation, 2026]	Advancing Artificial Intelligence Agent Ecosystems through the NSF PESOSE Program	agentic_ai_governance	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[for Disease Control and Prevention, 2026]	Considerations for Agentic Research in Public Health	agentic_ai_governance	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Standards and Technology, 2026f]	NIST AI RMF Playbook	ai_ethics_data_governance	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[OECD, 2024]	OECD AI Principles	ai_ethics_data_governance	international_standard	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[for Standardization, 2023b]	ISO/IEC 42001:2023 Artificial Intelligence Management System	ai_ethics_data_governance	international_standard	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[for Standardization, 2023a]	ISO/IEC 23894:2023 Artificial Intelligence Guidance on Risk Management	ai_ethics_data_governance	international_standard	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[of Europe, 2024]	Framework Convention on Artificial Intelligence	legal_oversight	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Office, 2025]	Copyright and Artificial Intelligence, Part 3: Generative AI Training	privacy_ip_governance	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Standards and Technology, 2020b]	Zero Trust Architecture, NIST SP 800-207	agentic_ai_governance	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Standards and Technology, 2025b]	Digital Identity Guidelines, NIST SP 800-63-4	agentic_ai_governance	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[IETF, 2025]	RFC 9700: Best Current Practice for OAuth 2.0 Security	agentic_ai_governance	internet_standard	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[IETF, 2023]	RFC 9449: OAuth 2.0 Demonstrating Proof of Possession	agentic_ai_governance	internet_standard	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Standards and Technology, 2012]	Guide for Conducting Risk Assessments, NIST SP 800-30 Rev. 1	legal_oversight	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[of Standards and Technology, 2018b]	Risk Management Framework for Information Systems and Organizations, NIST SP 800-37 Rev. 2	legal_oversight	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Standards and Technology, 2011a]	Information Security Continuous Monitoring, NIST SP 800-137	cyber_threat_intelligence	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Standards and Technology, 2011b]	Managing Information Security Risk, NIST SP 800-39	legal_oversight	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Standards and Technology, 2021]	Enhanced Security Requirements for Protecting Controlled Unclassified Information, NIST SP 800-172	counterintelligence_source_integrity	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Standards and Technology, 2022a]	Towards a Standard for Identifying and Managing Bias in Artificial Intelligence	ai_ethics_data_governance	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Committee, 2025]	STIX Version 2.1	cyber_threat_intelligence	international_standard	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Committee, 2021]	TAXII Version 2.1	cyber_threat_intelligence	international_standard	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[MITRE, 2026b]	MITRE ATT&CK Enterprise Matrix	cyber_threat_intelligence	research_standard	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Cybersecurity and Agency, 2026a]	Cross-Sector Cybersecurity Performance Goals	ics_ot_defense	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Cybersecurity and Agency, 2026e]	Secure by Design	agentic_ai_governance	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Cybersecurity and Agency, 2026d]	Known Exploited Vulnerabilities Catalog	cyber_threat_intelligence	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Agency, 2026b]	GEOINT Artificial Intelligence	osint_geoint	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[for Standardization, 2013]	ISO 19157:2013 Geographic Information - Data Quality	osint_geoint	international_standard	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Cybersecurity and Agency, 2026b]	Election Security	cognitive_influence_operations	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Organization, 2026c]	Countering Hybrid Threats	cognitive_influence_security	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[OECD, 2026c]	Disinformation and Misinformation	cognitive_influence_security	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Network, 2026b]	Beneficial Ownership Information Reporting	financial_economic_security	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Foreign Assets Control, 2019]	A Framework for OFAC Compliance Commitments	financial_economic_security	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Force, 2021]	Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers	financial_economic_security	international_standard	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[for International Settlements, 2021]	Fintech and the Digital Transformation of Financial Services	financial_economic_security	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Standards and Technology, 2017]	Framework for Cyber-Physical Systems: Volume 1, Overview	ics_ot_defense	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[of Standards and Technology, 2018a]	Protecting Information and System Integrity in Industrial Control System Environments, NIST SP 1800-10	ics_ot_defense	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Organization, 2026d]	Artificial Intelligence and Intellectual Property	privacy_ip_governance	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Standards and Technology, 2026k]	NIST Privacy Framework	privacy_ip_governance	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Standards and Technology, 2020a]	Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53 Rev. 5	legal_oversight	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Standards and Technology, 2024]	Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines, NIST IR 8477	legal_oversight	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Standards and Technology, 2024a]	Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations	agentic_ai_governance	official_primary	2026-05-21	annual	source URL, policy status, standard version, or legal text materially changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Commission, 2026b]	European AI Office	ai_conformity_compliance	official_primary	2026-05-22	quarterly	AI Office enforcement role, GPAI implementation, code status, or page ownership changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Commission, 2026h]	General-Purpose AI Code of Practice	ai_conformity_compliance	official_primary	2026-05-22	quarterly	GPAI code text, signatory status, Commission assessment, or AI Act timeline changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Commission, 2026a]	AI Act	ai_conformity_compliance	official_primary	2026-05-22	quarterly	AI Act implementation date, delegated act, guidance, or harmonised-standard status changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[for Standardization, 2025]	ISO/IEC 42005:2025 AI System Impact Assessment	ai_conformity_compliance	international_standard	2026-05-22	semiannual	ISO edition, corrigendum, lifecycle status, or linked package metadata changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[for Standardization, 2020]	ISO/IEC TR 24028:2020 Artificial Intelligence Trustworthiness Overview	ai_conformity_compliance	international_standard	2026-05-22	annual	ISO lifecycle stage, replacement, amendment, or JTC 1/SC 42 status changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Office, 2021]	Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities	ai_conformity_compliance	official_primary	2026-05-22	annual	GAO supplement, agency guidance, or framework revision changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[UNESCO, 2021]	Recommendation on the Ethics of Artificial Intelligence	human_rights_governance	international_standard	2026-05-22	annual	UNESCO implementation guidance, monitoring tool, or recommendation resource changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of the United Nations High Commissioner for Human Rights, 2026a]	Digital Space and Human Rights	human_rights_governance	official_primary	2026-05-22	semiannual	OHCHR thematic report, mandate, or digital-rights guidance updates	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[of the United Nations High Commissioner for Human Rights, 2026b]	The Right to Privacy in the Digital Age	human_rights_governance	official_primary	2026-05-22	semiannual	UN report, resolution, special procedure, or digital privacy guidance changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Europe, 2018]	Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data	human_rights_governance	official_primary	2026-05-22	annual	treaty status, ratification, explanatory report, or committee guidance changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[UNESCO, 2023]	Guidance for Generative AI in Education and Research	education_assessment	official_primary	2026-05-22	annual	UNESCO education guidance, generative-AI policy, or assessment recommendations change	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[UNESCO, 2024]	AI Competency Frameworks for Teachers and Students	education_assessment	official_primary	2026-05-22	annual	UNESCO framework publication, competency revision, or education resource update	Direct source URL verified against an official UNESCO source for AGEINT curriculum use as of 2026-05-22; automated liveness sweep on 2026-06-06 found the old article URL moved and recorded this likely successor URL, but UNESCO reset automated retrieval, so manual browser re-verification remains required.
[Report, 2026]	AI and Education	education_assessment	official_primary	2026-05-22	semiannual	GEM report, policy note, dashboard, or education indicator update	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[OECD, 2026b]	Artificial Intelligence in Education	education_assessment	official_primary	2026-05-22	semiannual	OECD topic update, education report, indicator, or policy brief changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Commission, 2026g]	Digital Education Action Plan 2021-2027	education_assessment	official_primary	2026-05-22	semiannual	Commission action-plan update, digital skills initiative, or education AI guidance changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Observatory, 2026b]	AI in the Public Sector	public_sector_agency_ai	official_primary	2026-06-06	semiannual	OECD public-sector theme, country practice, policy guidance, or measurement update	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use; URL refreshed 2026-06-06 after liveness check.
[GovTech and Team, 2026]	Artificial Intelligence Working Group	public_sector_agency_ai	official_primary	2026-05-22	semiannual	working-group membership, policy instrument, repository, or public-sector case update	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Bank, 2026]	GovTech: Putting People First	public_sector_agency_ai	official_primary	2026-05-22	semiannual	GovTech Maturity Index, program priority, case repository, or public-sector digital update	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Administration, 2026]	AI Guide for Government	public_sector_agency_ai	official_primary	2026-05-22	quarterly	federal AI guidance, agency practice, resource hub, or policy source changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Commission, 2026e]	European Data Governance Act	cross_border_data_spaces	official_primary	2026-05-22	semiannual	Data Governance Act application, EDIB guidance, data intermediary, or data altruism update	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Commission, 2026d]	Data Act Explained	cross_border_data_spaces	official_primary	2026-05-22	semiannual	Data Act implementation, FAQs, interoperability guidance, or Commission simplification changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Commission, 2026c]	Common European Data Spaces	cross_border_data_spaces	primary	2026-05-22	semiannual	data-space rollout, domain list, reference architecture, or interoperability update	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Commission, 2026f]	A European Strategy for Data	cross_border_data_spaces	primary	2026-05-22	semiannual	European data strategy update, policy package change, or data-space program update	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Consortium, 2023a]	Web of Things (WoT) Architecture 1.1	agent_interoperability_standards	standards	2026-05-22	annual	W3C Recommendation, errata, successor specification, or WoT architecture update	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Consortium, 2023c]	Web of Things (WoT) Thing Description 1.1	agent_interoperability_standards	standards	2026-05-22	annual	W3C Recommendation, errata, successor specification, or thing-description vocabulary update	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Consortium, 2023b]	Web of Things (WoT) Discovery	agent_interoperability_standards	standards	2026-05-22	annual	W3C Recommendation, errata, successor specification, or discovery security update	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Initiative, 2026b]	OpenAPI Specification	agent_interoperability_standards	standards	2026-05-22	semiannual	OpenAPI version, schema revision, or specification publication changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Consortium, 2025b]	Verifiable Credentials Data Model v2.0	agent_interoperability_standards	standards	2026-05-22	annual	W3C Recommendation, errata, implementation report, or data-model update	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Consortium, 2022]	Decentralized Identifiers (DIDs) v1.0	agent_interoperability_standards	international_standard	2026-05-22	annual	W3C Recommendation, errata, DID method guidance, or registry changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Force, 2022]	RFC 9110: HTTP Semantics	agent_interoperability_standards	international_standard	2026-05-22	annual	RFC update, errata, bis document, or HTTP specification status changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Organization, 2026a]	Artificial Intelligence	workforce_governance	official_primary	2026-05-22	semiannual	ILO AI topic update, report, policy note, or labour-market evidence update	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Organization and Nations, 2024]	Mind the AI Divide: Shaping a Global Perspective on the Future of Work	workforce_governance	official_primary	2026-05-22	annual	ILO/UN report revision, follow-up data, or labour-market exposure model update	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Organization, 2019]	Global Commission on the Future of Work	workforce_governance	official_primary	2026-05-22	annual	ILO centenary initiative, commission follow-up, decent-work agenda, or policy update	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Observatory, 2026a]	AI and Work	workforce_governance	official_primary	2026-06-06	semiannual	OECD AI work theme, labour indicator, report, or policy-dashboard update	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use; URL refreshed 2026-06-06 after liveness check.
[Consortium, 2013b]	PROV Overview	model_data_provenance	international_standard	2026-05-22	annual	W3C PROV errata, successor work, or provenance vocabulary update	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Consortium, 2013a]	PROV-O: The PROV Ontology	model_data_provenance	international_standard	2026-05-22	annual	W3C Recommendation errata, ontology update, or provenance best-practice change	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Consortium, 2024]	Data Catalog Vocabulary (DCAT) Version 3	model_data_provenance	international_standard	2026-05-22	annual	W3C Recommendation, vocabulary term, errata, or data-catalog practice update	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Consortium, 2017]	Data on the Web Best Practices	model_data_provenance	international_standard	2026-05-22	annual	W3C best-practice update, errata, or linked data publication guidance change	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Standards and Technology, 2026h]	NIST Big Data Interoperability Framework	model_data_provenance	official_primary	2026-06-06	annual	NIST big-data framework volume, version, roadmap, or program update	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use; URL refreshed 2026-06-06 after liveness check.
[DataCite, 2026]	DataCite Metadata Schema	model_data_provenance	research_standard	2026-05-22	annual	schema version, DOI metadata property, controlled vocabulary, or relation-type update	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[for Content Provenance and Authenticity, 2026]	C2PA Specifications	model_data_provenance	technical_standard	2026-06-06	semiannual	C2PA specification version, assertion vocabulary, verification model, or threat update	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use; URL refreshed 2026-06-06 after liveness check.
[Initiative, 2026c]	WCAG 2 Overview	accessibility_digital_inclusion	standard	2026-05-22	semiannual	WCAG publication, conformance guidance, or public-sector accessibility requirement changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[CAST, 2024]	CAST Universal Design for Learning Guidelines version 3.0	accessibility_digital_inclusion	educational_guidance	2026-05-22	annual	UDL guideline version, citation guidance, or inclusive-learning practice changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Justice, 2024]	Fact Sheet: New Rule on the Accessibility of Web Content and Mobile Apps Provided by State and Local Governments	accessibility_digital_inclusion	official_primary	2026-05-22	quarterly	ADA Title II rule, Federal Register update, compliance date, or DOJ guidance changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Board, 2026]	What is a Data Protection Impact Assessment and When Is This Mandatory?	rights_impact_privacy	official_primary	2026-05-22	semiannual	EDPB DPIA guidance, GDPR interpretation, SME guide, or high-risk processing examples change	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Board, 2018]	Endorsed WP29 Guidelines	rights_impact_privacy	official_primary	2026-05-22	semiannual	EDPB guideline endorsement, supersession, or GDPR guidance page changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[OECD, 2015]	Recommendation of the Council on Public Procurement	procurement_vendor_governance	official_primary	2026-05-22	annual	OECD legal instrument revision, public procurement toolkit update, or procurement policy change	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Partnership, 2026]	Open Contracting Data Standard	procurement_vendor_governance	technical_standard	2026-05-22	annual	OCDS schema, documentation version, governance page, or procurement transparency model changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Standards and Technology, 2025d]	Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile	agent_incident_response	official_primary	2026-05-22	semiannual	NIST SP 800-61 revision, CSF 2.0 community profile update, or incident-response terminology changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[for Cybersecurity, 2020]	Artificial Intelligence Cybersecurity Challenges	ai_red_team_assurance	official_primary	2026-05-22	annual	ENISA AI threat landscape, AI cybersecurity guidance, or EU cybersecurity policy changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Standards and Technology, 2026g]	AI Research: Security and Resilience	ai_red_team_assurance	official_primary	2026-05-22	quarterly	NIST AI security report, adversarial machine learning taxonomy, or AI RMF security update changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Standards and Technology, 2026d]	NIST AI Resource Center	ai_red_team_assurance	official_primary	2026-05-22	quarterly	AI RMF revision, playbook revision, AIRC technical reports, or TEVV resources change	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[OECD, 2017]	Recommendation of the Council on Open Government	public_sector_transparency	official_primary	2026-05-22	annual	OECD open government legal instrument, public governance guidance, or civic-space update changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Consortium, 2025a]	Verifiable Credential Data Integrity 1.0	model_data_provenance	technical_standard	2026-05-22	semiannual	W3C VC Data Integrity recommendation, errata, cryptosuite, or implementation report changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Margaret Mitchell and Gebru, 2019]	Model Cards for Model Reporting	model_card_reporting	scholarly	2026-05-22	annual	model reporting practice, model-card schema, or scholarly consensus changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Timnit Gebru and Crawford, 2021]	Datasheets for Datasets	dataset_documentation	scholarly	2026-05-22	annual	dataset documentation practice, data-card schema, or scholarly consensus changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Service, 2025b]	Algorithmic Transparency Recording Standard Hub	algorithmic_transparency_reporting	official_primary	2026-05-22	quarterly	ATRS template, scope policy, central government mandate, or publication guidance changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Service, 2025a]	Guidance for Organisations Using the Algorithmic Transparency Recording Standard	algorithmic_transparency_reporting	official_primary	2026-05-22	quarterly	ATRS completion guidance, repository process, or publication policy changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Standards and Technology, 2024a]	Secure Software Development Practices for Generative AI and Dual-Use Foundation Models	secure_release_change_control	official_primary	2026-05-22	semiannual	NIST SSDF, SP 800-218A, generative-AI profile, or AI secure-development practice changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Board, 2017]	Revised 508 Standards and 255 Guidelines	learner_support_accessibility	official_primary	2026-05-22	semiannual	federal ICT accessibility standard, accessibility rule, exception, or documentation requirement changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Standards and Technology, 2025a]	Assessing Risks and Impacts of AI (ARIA): Pilot Evaluation Report	assurance_evaluation_validation	official_primary	2026-05-22	quarterly	ARIA evaluation program, pilot report, scenario design, or AI measurement guidance changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Archives and Administration, 2026a]	Inventory of NARA Artificial Intelligence (AI) Use Cases	records_retention_disposition_liability	official_primary	2026-05-22	quarterly	NARA AI use-case inventory, agency AI use-case disclosure, records policy, or FOIA workflow changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of the President, 2025a]	M-25-21: Accelerating Federal Use of AI through Innovation, Governance, and Public Trust	risk_exception_governance	official_primary	2026-05-22	quarterly	OMB federal AI governance memo, agency strategy requirement, traceability, or monitoring guidance changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[of the President, 2025b]	M-25-22: Driving Efficient Acquisition of Artificial Intelligence in Government	procurement_performance_monitoring	official_primary	2026-05-22	quarterly	OMB AI acquisition memo, QASP guidance, solicitation transparency, or monitoring requirement changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Standards and Technology, 2024e]	Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile	assurance_evaluation	official_primary	2026-06-11	semiannual	NIST AI 600-1 revision, AI RMF profile update, generative-AI risk guidance, or evaluation action changes	Direct NIST AI 600-1 PDF and NIST publication landing page verified live 2026-06-11 for GenAI Profile scope and AI RMF alignment.
[Cybersecurity and Agency, 2024a]	AI Red Teaming: Applying Software TEVV for AI Evaluations	ai_red_team_assurance	official_primary	2026-05-22	semiannual	CISA AI red-teaming, TEVV, security-evaluation, or AI-testing guidance changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Cybersecurity et al., 2025b]	AI Data Security: Best Practices for Securing Data Used to Train and Operate AI Systems	model_data_provenance	official_primary	2026-06-11	semiannual	CISA, NSA, FBI, or partner AI data-security lifecycle guidance changes	Direct official CISA/NSA/FBI partner PDF verified live 2026-06-11; executive summary covers AI data security, lifecycle stages, integrity risks, and best practices.
[of Standards and Technology, 2026e]	Concept Note: AI RMF Profile on Trustworthy AI in Critical Infrastructure	assurance_evaluation	official_primary	2026-05-22	quarterly	NIST AI RMF critical-infrastructure profile concept, draft, final profile, or public-comment update	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[for Economic Co-operation and Development, 2025b]	Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions	public_sector_transparency	official_primary	2026-05-22	semiannual	OECD government AI governance, enabler, guardrail, engagement, or public-sector use-case update	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Archives and Administration, 2025]	NARA 2025 AI Compliance Plan	records_retention_auditability	official_primary	2026-05-22	semiannual	NARA AI compliance plan, records policy, AI use-case inventory, audit, or federal AI governance update	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[of Canada Secretariat, 2026a]	Guide on the Use of Agentic Artificial Intelligence	public_sector_agentic_ai	official_primary	2026-05-24	quarterly	Canada agentic-AI guide, public-sector AI policy, autonomy control, transparency, or monitoring guidance changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Canada Secretariat, 2026b]	Algorithmic Impact Assessment tool	rights_impact_privacy	official_primary	2026-05-24	quarterly	Algorithmic Impact Assessment tool, directive, scoring, mitigation, or government automated-decision policy changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Canada Secretariat, 2025]	Canada launches first register of AI uses in federal government	public_sector_transparency	official_primary	2026-05-24	quarterly	Canada AI register launch, register schema, public inventory, disclosure requirement, or federal AI-use publication changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Canada, 2025]	AI Strategy for the Federal Public Service 2025-2027: Priority areas	workforce_governance	official_primary	2026-05-24	quarterly	Canada AI Strategy 2025-2027 priority, implementation, workforce, governance, or public-service AI adoption changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[for Economic Co-operation and Development, 2026b]	AI risks and incidents	agent_incident_response	official_primary	2026-05-24	quarterly	OECD AI incident monitor, risk taxonomy, AI incident topic, or AI hazard reporting changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[for Economic Co-operation and Development, 2025a]	Towards a common reporting framework for AI incidents	agent_incident_response	official_primary	2026-05-24	quarterly	OECD AI incident reporting framework, criteria, DOI landing page, implementation, or interoperable incident-reporting guidance changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Nations, 2024]	Global Digital Compact	accessibility_digital_inclusion	official_primary	2026-05-24	semiannual	UN Global Digital Compact implementation, adopted text, digital cooperation portal, AI governance, or digital-inclusion update	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[of Standards and Technology, 2026i]	Dioptra	ai_red_team_assurance	official_primary	2026-05-24	quarterly	NIST Dioptra release, documentation, testbed capability, AI measurement, or adversarial-evaluation update	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Cybersecurity et al., 2024]	Joint Guidance on Deploying AI Systems Securely	secure_release_change_control	official_primary	2026-05-24	semiannual	CISA or partner AI deployment guidance, secure configuration, monitoring, release, or incident-management update	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Cybersecurity and Agency, 2025b]	Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products	procurement_vendor_governance	official_primary	2026-05-24	semiannual	CISA Secure by Demand, OT procurement, vendor security, priority consideration, or owner/operator guidance changes	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Cybersecurity et al., 2025a]	CISA and Partners Release Asset Inventory Guidance to Strengthen Operational Technology Security	records_retention_auditability	official_primary	2026-05-24	semiannual	CISA OT asset inventory guidance, partner release, asset-record field, inventory process, or OT security visibility update	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[Cybersecurity and Agency, 2025a]	Creating and Maintaining a Definitive View of Your Operational Technology (OT) Architecture	assurance_evaluation_validation	official_primary	2026-05-24	semiannual	CISA OT architecture guidance, architecture record, communication map, definitive-view process, or change-control recommendation update	Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.
[of Excellence, 2026]	New CCDCOE Research Reconceptualises Cognitive Warfare	human_rights_governance	official_primary	2026-05-22	semiannual	CCDCOE cognitive warfare research, systemic-invariants model, cognitive-decoherence framing, or NATO CoE cognitive-security publication changes	Direct source URL verified live (HTTP 200, on-topic CCDCOE cognitive-warfare research) for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Agency, 2024a]	Intrinsic Cognitive Security (ICS)	assurance_evaluation	official_primary	2026-05-22	semiannual	DARPA ICS program scope, formal-methods approach, cognitive-attack taxonomy, or CAMP knowledgebase publication changes	Direct source URL verified live (HTTP 200, on-topic DARPA ICS program page) for AGEINT curriculum use.
[Alliance, 2025a]	Introducing Cognitive Degradation Resilience (CDR): A Framework for Safeguarding Agentic AI Systems from Systemic Collapse	agent_incident_response	official_primary	2026-05-22	quarterly	CSA CDR framework, degradation-stage model, QSAF-BC controls, health-probe guidance, or agentic-AI resilience publication changes	Direct source URL verified live (HTTP 200, on-topic CSA CDR framework) for AGEINT curriculum use.
[Alliance, 2025b]	Agentic AI Threat Modeling Framework: MAESTRO	ai_red_team_assurance	official_primary	2026-05-22	quarterly	CSA MAESTRO framework, seven-layer model, per-layer mitigation guidance, or agentic-AI threat-modeling publication changes	Direct source URL verified live (HTTP 200, on-topic CSA MAESTRO framework) for AGEINT curriculum use.
[Mandel and Tetlock, 2018]	Correcting Judgment Correctives in National Security Intelligence	education_assessment	scholarly_peer_reviewed	2026-05-22	annual	Updated peer-reviewed work on analytic debiasing, SAT validation, noise-versus-bias evidence, or replacement of the PMC landing record	Direct source URL verified live (HTTP 200, on-topic NIH PMC peer-reviewed article) for AGEINT curriculum use.
[arXiv preprint authors, 2025a]	Agentic AI Security: Threats, Defenses, Evaluation, and Open Challenges	ai_red_team_assurance	scholarly_preprint	2026-05-22	quarterly	New arXiv version of the agentic-AI security survey, revised threat taxonomy, defense catalog, or evaluation-methodology updates	Direct source URL verified live (HTTP 200, on-topic arXiv agentic-AI security survey) for AGEINT curriculum use.
[Anthropic, 2024]	Building Effective AI Agents	agent_interoperability_standards	frontier_lab_research	2026-05-22	semiannual	Anthropic Building Effective Agents updates, revised pattern taxonomy, or successor agent-architecture guidance changes	Direct source URL verified live (HTTP 200, on-topic Anthropic agent-architecture research) for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[DeepMind and Research, 2026]	Architecting Trust in Artificial Epistemic Agents	model_data_provenance	frontier_lab_research	2026-05-22	annual	New arXiv version of the epistemic-agent trust paper, revised trust desiderata, provenance architecture, or successor DeepMind publication changes	Direct source URL verified live (HTTP 200, on-topic DeepMind epistemic-agent arXiv paper) for AGEINT curriculum use.
[Lee and Tiwari, 2024]	Prompt Infection: LLM-to-LLM Prompt Injection within Multi-Agent Systems	agent_incident_response	scholarly_preprint	2026-05-22	annual	New arXiv version of Prompt Infection, revised propagation model, or successor multi-agent injection defense research changes	Direct source URL verified live (HTTP 200, on-topic arXiv prompt-infection paper) for AGEINT curriculum use.
[arXiv preprint authors, 2025b]	Systems Security Foundations for Agentic Computing	secure_release_change_control	scholarly_preprint	2026-05-22	annual	New arXiv version of Systems Security Foundations for Agentic Computing, revised privilege model, or successor agentic-security-foundations research changes	Direct source URL verified live (HTTP 200, on-topic arXiv agentic systems-security paper) for AGEINT curriculum use.
[Initiative), 2025]	Agentic AI – Threats and Mitigations	ai_red_team_assurance	official_primary	2026-05-22	quarterly	OWASP Agentic Security Initiative whitepaper revisions, threat-model updates, or new agentic threats-and-mitigations guidance changes	Direct source URL verified live (HTTP 200, on-topic OWASP agentic threats-and-mitigations resource) for AGEINT curriculum use.
[Alliance, 2026]	Securing Autonomous AI Agents	procurement_vendor_governance	official_primary	2026-05-22	quarterly	CSA securing-autonomous-AI-agents survey revisions, identity-governance findings, or agent IAM-readiness data updates	Direct source URL verified live (HTTP 200, on-topic CSA securing-autonomous-AI-agents artifact) for AGEINT curriculum use.
[Initiative, 2026a]	CSA Research Note: NIST AI Agent Red-Teaming Standards (March 2026)	ai_red_team_assurance	official_primary	2026-05-22	quarterly	CSA/NIST AI agent red-teaming standards note revisions, CAISI findings, adversarial-ML taxonomy, or red-team standard updates	Direct source URL verified live (HTTP 200, on-topic CSA/NIST AI agent red-teaming standards note) for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[United Nations University, 2026]	Why Agentic AI Needs Boundaries Before Freedom	human_rights_governance	official_primary	2026-05-22	semiannual	UNU Macau agentic-AI governance publications, minimum-privilege doctrine, oversight guidance, or UN academic agentic-AI policy changes	Direct source URL verified live (HTTP 200, on-topic UNU Macau agentic-AI governance analysis) for AGEINT curriculum use.
[of Standards and Technology, 2024b]	Reducing Risks Posed by Synthetic Content: An Overview of Technical Approaches to Digital Content Transparency	model_data_provenance	official_primary	2026-06-11	annual	NIST AI 100-4 revision, synthetic-content transparency standard, provenance technology, watermarking guidance, or digital-content policy materially changes	Direct NIST AI 100-4 PDF and publication landing page verified live 2026-06-11; report covers provenance, labeling, watermarking, detection, testing, auditing, and maintenance.
[of Standards and Technology, 2024c]	A Plan for Global Engagement on AI Standards	ai_conformity_compliance	official_primary	2026-06-06	annual	NIST global AI standards plan, standards-development priorities, international AI standards coordination, or conformity-assessment guidance changes	Direct source URL verified live (HTTP 200 PDF, title metadata and first pages on-topic) for AGEINT curriculum use.
[U.S. AI Safety Institute and Technology, 2024]	Managing Misuse Risk for Dual-Use Foundation Models, NIST AI 800-1 Initial Public Draft	ai_red_team_assurance	official_draft	2026-06-06	quarterly	NIST AI 800-1 finalization, draft revision, U.S. AI Safety Institute misuse-risk framework, dual-use foundation-model safeguard guidance, or evaluation practice changes	Direct source URL verified live (HTTP 200 PDF, title metadata and first pages on-topic); Draft status retained explicitly for AGEINT curriculum use.
[Group and Panel, 2026]	International AI Safety Report 2026	assurance_evaluation	official_scientific_synthesis	2026-06-12	annual	International AI Safety Report release, extended policymaker summary, expert advisory panel update, or major frontier-AI safety evidence changes	Direct official report landing page verified live (HTTP 200, International AI Safety Report 2026 page on-topic); the official PDF and arXiv record remain secondary evidence when needed.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Project, 2025c]	Specification - Model Context Protocol	agent_interoperability	official_standards	2026-06-11	quarterly	MCP specification version, protocol capability model, authorization profile, transport guidance, or security model changes	Direct official MCP specification page verified live 2026-06-11; security and trust language retained as a boundary, not a deployment guarantee.
[Project, 2025b]	Security Best Practices - Model Context Protocol	secure_release_change	official_primary	2026-06-11	quarterly	MCP security guidance, authorization/security best-practice page, confused-deputy mitigation, token-handling guidance, or tool-consent requirements change	Direct official MCP security best-practices page verified live 2026-06-11; page describes security considerations, attack vectors, and best practices for MCP implementations.
[Project, 2025a]	Agent2Agent (A2A) Protocol	agent_interoperability	official_standards	2026-06-06	quarterly	A2A protocol version, agent-discovery model, security profile, transport model, or governance home changes	Direct source URL verified live (HTTP 200, official A2A protocol documentation with on-topic description metadata) for AGEINT curriculum use.
[Centre and international partners, 2024]	Guidelines for Secure AI System Development	secure_release_change	official_primary	2026-06-06	annual	NCSC secure-AI-development guidance, joint-authority updates, secure-by-design AI controls, supply-chain guidance, or provider responsibility model changes	Direct source URL verified live (HTTP 200, on-topic NCSC secure-AI-development guidance page) for AGEINT curriculum use.
[MITRE, 2026d]	D3FEND Matrix	assurance_evaluation	research_evidence	2026-06-06	quarterly	D3FEND matrix, countermeasure taxonomy, ATT&CK relationship model, ontology release, or defensive-control mapping changes	Direct source URL verified live (HTTP 200, official MITRE D3FEND page with on-topic title and description metadata) for AGEINT curriculum use.
[Open, 2022]	Common Security Advisory Framework Version 2.0	records_retention_traceability	technical_standard	2026-06-12	annual	CSAF version, errata, vulnerability-advisory schema, product-status vocabulary, remediation field, or OASIS standard status changes	Direct canonical OASIS OS HTML source URL verified live (HTTP 200, CSAF Version 2.0 OASIS Standard page on-topic) for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Project, 2026a]	CycloneDX Specification Overview	model_data_provenance	security_standard	2026-06-06	quarterly	CycloneDX specification version, BOM type, vulnerability extension, AI/component metadata, or supply-chain provenance guidance changes	Direct source URL verified live (HTTP 200, official CycloneDX specification overview page) for AGEINT curriculum use.
[SPDX Project, 2024]	SPDX Specification 3.0.1	model_data_provenance	technical_standard	2026-06-06	annual	SPDX specification version, profile model, security/licensing field, SBOM practice, or Linux Foundation governance update changes	Direct source URL verified live (HTTP 200, official SPDX Specification 3.0.1 page with SBOM description metadata) for AGEINT curriculum use.
[of Standards and Technology, 2026j]	OSCAL - Open Security Controls Assessment Language	records_retention_auditability	primary	2026-06-06	quarterly	OSCAL model version, NIST control catalog, assessment result schema, component definition, or compliance automation guidance changes	Direct source URL verified live (HTTP 200, official NIST OSCAL page) for AGEINT curriculum use.
[chain Levels for Software Artifacts Project, 2026]	SLSA Specification	secure_release_change_control	security_standard	2026-06-06	quarterly	SLSA specification version, provenance model, build-level requirement, dependency track, or supply-chain security guarantee changes	Direct source URL verified live (HTTP 200, official SLSA v1.1 specification page with on-topic description metadata) for AGEINT curriculum use.
[in-toto Project, 2026]	in-toto	secure_release_change_control	security_standard	2026-06-06	quarterly	in-toto specification, attestation format, layout model, supply-chain integration, or provenance tooling changes	Direct source URL verified live (HTTP 200, official in-toto project page) for AGEINT curriculum use.
[Project, 2026c]	Overview - Sigstore	secure_release_change_control	security_standard	2026-06-06	quarterly	Sigstore documentation, signing workflow, transparency log, identity binding, provenance verification, or project governance changes	Direct source URL verified live (HTTP 200, official Sigstore documentation overview page) for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Friston, 2010]	The free-energy principle: a unified brain theory?	cognitive_active_inference	scholarly_peer_review	2026-06-08	annual	source URL, DOI, edition/standard version, or claim scope materially changes	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Friston, 2017]	Active Inference: A Process Theory	cognitive_active_inference	scholarly_peer_review	2026-06-08	annual	source URL, DOI, edition/standard version, or claim scope materially changes	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Da Costa, 2020]	Active inference on discrete state-spaces: A synthesis	cognitive_active_inference	scholarly_peer_review	2026-06-08	annual	source URL, DOI, edition/standard version, or claim scope materially changes	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Parr, 2022]	Active Inference: The Free Energy Principle in Mind, Brain, and Behavior	cognitive_active_inference	scholarly_textbook	2026-06-08	annual	source URL, DOI, edition/standard version, or claim scope materially changes	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Yao, 2023a]	ReAct: Synergizing Reasoning and Acting in Language Models	agentic_ai_governance	scholarly_preprint	2026-06-08	annual	source URL, DOI, edition/standard version, or claim scope materially changes	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Shinn, 2023]	Reflexion: Language Agents with Verbal Reinforcement Learning	agentic_ai_governance	scholarly_preprint	2026-06-08	annual	source URL, DOI, edition/standard version, or claim scope materially changes	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Park, 2023]	Generative Agents: Interactive Simulacra of Human Behavior	agentic_ai_governance	scholarly_peer_review	2026-06-08	annual	source URL, DOI, edition/standard version, or claim scope materially changes	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Wei, 2022]	Chain-of-Thought Prompting Elicits Reasoning in Large Language Models	agentic_ai_governance	scholarly_preprint	2026-06-08	annual	source URL, DOI, edition/standard version, or claim scope materially changes	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Schick, 2023]	Toolformer: Language Models Can Teach Themselves to Use Tools	agentic_ai_governance	scholarly_preprint	2026-06-08	annual	source URL, DOI, edition/standard version, or claim scope materially changes	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Wooldridge, 1995]	Intelligent agents: theory and practice	agentic_ai_governance	scholarly_peer_review	2026-06-08	annual	source URL, DOI, edition/standard version, or claim scope materially changes	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Wooldridge, 2009]	An Introduction to MultiAgent Systems, 2nd Edition	agentic_ai_governance	scholarly_textbook	2026-06-08	annual	source URL, DOI, edition/standard version, or claim scope materially changes	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Burkett, 2013]	An Alternative Framework for Agent Recruitment: From MICE to RASCLS	counterintelligence_officer_integrity	official_publication	2026-06-08	annual	source URL, DOI, edition/standard version, or claim scope materially changes	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Meissner, 2017]	Developing an Evidence-Based Perspective on Interrogation: A Review of the U.S. Government's High-Value Detainee Interrogation Group Research Program	counterintelligence_officer_integrity	scholarly_peer_review	2026-06-08	annual	source URL, DOI, edition/standard version, or claim scope materially changes	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Brimbal, 2020]	Developing Rapport and Trust in the Interrogative Context: An Empirically Supported Alternative	counterintelligence_officer_integrity	scholarly_peer_review	2026-06-08	annual	source URL, DOI, edition/standard version, or claim scope materially changes	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Nunan, 2020]	Eliciting human intelligence: police source handlers' perceptions and experiences of rapport during covert human intelligence sources (CHIS) interactions	counterintelligence_source_vetting	scholarly_peer_review	2026-06-08	annual	source URL, DOI, edition/standard version, or claim scope materially changes	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Kelly, 2013]	A Taxonomy of Interrogation Methods	counterintelligence_source_vetting	scholarly_peer_review	2026-06-08	annual	source URL, DOI, edition/standard version, or claim scope materially changes	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Pherson, 2014a]	Structured Analytic Techniques for Intelligence Analysis	analytic_tradecraft	scholarly_textbook	2026-06-08	annual	source URL, DOI, edition/standard version, or claim scope materially changes	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[of Standards and , NIST]	FIPS 197: Advanced Encryption Standard (AES)	cyber_threat_intelligence	technical_standard	2026-06-08	annual	source URL, DOI, edition/standard version, or claim scope materially changes	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[of Standards and , NIST]	FIPS 186-5: Digital Signature Standard (DSS)	cyber_threat_intelligence	technical_standard	2026-06-08	annual	source URL, DOI, edition/standard version, or claim scope materially changes	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[of Standards and , NIST]	FIPS 180-4: Secure Hash Standard (SHS)	cyber_threat_intelligence	technical_standard	2026-06-08	annual	source URL, DOI, edition/standard version, or claim scope materially changes	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[, NIST]	NIST SP 800-57 Part 1 Rev. 5: Recommendation for Key Management, Part 1: General	cyber_threat_intelligence	technical_standard	2026-06-08	annual	source URL, DOI, edition/standard version, or claim scope materially changes	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[McGuire, 1961]	Resistance to persuasion conferred by active and passive prior refutation of the same and alternative counterarguments	cognitive_influence_security	scholarly_peer_review	2026-06-08	annual	source URL, DOI, edition/standard version, or claim scope materially changes	Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.
[Mahima Pushkarna and Kjartansson, 2022]	Data Cards: Purposeful and Transparent Dataset Documentation for Responsible AI	dataset_documentation	scholarly_peer_review	2026-06-09	annual	Data Cards paper, ACM record, arXiv record, dataset-documentation practice, or scholarly consensus materially changes	Direct arXiv source URL verified live 2026-06-09 with title, authors, abstract, and ACM FAccT 2022 metadata matching the cited Data Cards paper.
[Christopher L. Buckley and Seth, 2017]	The Free Energy Principle for Action and Perception: A Mathematical Review	cognitive_active_inference	scholarly_preprint	2026-06-10	annual	arXiv record, DOI record, active-inference review literature, or cited mathematical formulation materially changes	Direct arXiv source URL verified live 2026-06-10 with title, authors, submission date, abstract, and DOI metadata matching the cited mathematical review.
[Melissa L. Rethlefsen and the PRISMA-S Group, 2021]	PRISMA-S: An Extension to the PRISMA Statement for Reporting Literature Searches in Systematic Reviews	source_construction_reporting	scholarly_peer_review	2026-06-10	annual	PRISMA-S guideline, PRISMA statement, systematic-review reporting practice, or journal record materially changes	Direct journal landing page verified live 2026-06-10 with title, authors, publication date, journal metadata, and abstract describing the 16-item PRISMA-S checklist.
[Kai Greshake and Fritz, 2023]	Not What You've Signed Up For: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection	agentic_ai_security	scholarly_preprint	2026-06-10	annual	arXiv record, DOI record, indirect prompt-injection literature, agentic tool-security guidance, or threat taxonomy materially changes	Direct arXiv source URL verified live 2026-06-10 with title, authors, submission and revision metadata, DOI, and abstract describing indirect prompt-injection attacks.
[of Standards and Technology, 2026b]	Practices for Automated Benchmark Evaluations of Language Models and AI Agent Systems, NIST AI 800-2 Initial Public Draft	assurance_evaluation	official_standard	2026-06-11	quarterly	NIST AI 800-2 draft revision, final publication, benchmark evaluation practice update, public comment resolution, or agent-system evaluation guidance changes	Direct NIST AI 800-2 PDF and NIST announcement verified live 2026-06-11; draft status retained explicitly for AGEINT curriculum use.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[for Economic Co-operation and Development, 2026a]	The Agentic AI Landscape and Its Conceptual Foundations	agent_interoperability_standards_analysis	official_publication	2026-06-11	semiannual	OECD agentic AI paper, definition update, policy analysis, uptake data, or OECD AI-system definition guidance changes	Direct OECD publication page verified live 2026-06-11; abstract describes definition comparison, OECD AI-system mapping, and uptake trends.
[Agency, 2026i]	Model Context Protocol (MCP): Security Design Considerations for Organizations	secure_release_change_control	official_publication	2026-06-11	quarterly	NSA MCP security guidance, MCP protocol security profile, implementation vulnerability guidance, or secure-adoption recommendations change	Direct NSA PDF URL verified live 2026-06-11; guidance frames MCP security adoption controls and recommendations for organizations.
[Jon Roozenbeek and Lewandowsky, 2022]	Psychological Inoculation Improves Resilience Against Misinformation on Social Media	cognitive_resilience_scholarly_peer_review	scholarly_publication	2026-06-11	annual	Science Advances record, DOI metadata, replication literature, meta-analysis, or evidence boundary materially changes	Direct Science Advances DOI page verified live 2026-06-11 with title, journal, DOI, and abstract-level claim that inoculation campaigns improved misinformation resilience at scale.
[for the Study of Intelligence, 2002]	Sherman Kent and the Profession of Intelligence Analysis	analytic_tradecraft_foundations	official_publication	2026-06-11	annual	Refresh if CIA replaces the PDF or publishes a newer CSI Kent/tradecraft history.	Direct CIA PDF verified live 2026-06-11; use for Kent-as-profession and standards claims, not for contemporary agency policy.
[for the Study of Intelligence, 1994]	Sherman Kent's Final Thoughts on Analyst-Policymaker Relations	analytic_tradecraft_foundations	official_publication	2026-06-11	annual	Refresh if CIA replaces the PDF or publishes a newer CSI version.	Direct CIA PDF verified live 2026-06-11; use for warning and analyst-policy boundary framing.
[Wohlstetter, 1962]	Pearl Harbor: Warning and Decision	warning_intelligence_scholarly_publisher	scholarly_publication	2026-06-11	annual	Refresh if publisher metadata or edition details change.	Stanford University Press publisher page verified live 2026-06-11; use as classic warning theory, not as current doctrine.
[Grabo, 1972]	Handbook of Warning Intelligence	warning_intelligence_official_declassified	official_publication	2026-06-11	annual	Refresh if CIA Reading Room record or declassification file changes.	CIA Reading Room PDF verified live 2026-06-11; use for historical warning concepts, not operational collection instructions.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Congress, 2004]	Intelligence Reform and Terrorism Prevention Act of 2004	intelligence_failure_postmortem	official_primary	2026-06-11	biennial	Refresh if GovInfo metadata or statutory-citation links change.	GovInfo public law landing page verified live 2026-06-11; use for statutory reform context, not implementation-detail claims.
[on Terrorist Attacks Upon the United States, 2004]	The 9/11 Commission Report	intelligence_failure_postmortem	official_primary	2026-06-11	biennial	Refresh if official commission site or report URL changes.	Official commission PDF verified live 2026-06-11; use for postmortem and reform context, not as a one-size failure formula.
[on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005]	Report to the President of the United States: The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction	intelligence_failure_postmortem	official_primary	2026-06-11	biennial	Refresh if official hosted PDF or archival record changes.	Defense policy-hosted official report PDF verified live 2026-06-11; use for assumptions/evidence and analytic-failure context.
[Transformation, 2017]	Alternative Analysis Handbook	analytic_tradecraft_guidance	official_primary	2026-06-11	annual	Refresh if NATO publishes a newer alternative-analysis handbook or relocates the PDF.	NATO ACT PDF verified live 2026-06-11; use as doctrine/practice guidance, not empirical proof of SAT effectiveness.
[Bruce, 2016]	Assessing the Value of Structured Analytic Techniques in the U.S. Intelligence Community	sat_evaluation_evidence	policy_research_report	2026-06-15	annual	Refresh if RAND publishes a newer SAT evaluation synthesis or corrects report metadata.	RAND report metadata and PDF URL verified again on 2026-06-15 from the RAND publication record and direct PDF URL; use for evaluation-limit claims and evidence-boundary framing.
[Alexandru Marcoci and Jonas, 2019]	Better Together: Reliable Application of the Post-9/11 and Post-Iraq US Intelligence Tradecraft Standards Requires Collective Analysis	sat_evaluation_evidence	scholarly_peer_review	2026-06-11	annual	Refresh if journal metadata, correction, or retraction status changes.	Frontiers open article verified live 2026-06-11; use for tradecraft-rating reliability and collective review claims.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Barnes and Mandel, 2014]	Accuracy of Forecasts in Strategic Intelligence	forecasting_calibration_evidence	scholarly_peer_reviewed	2026-06-11	annual	Refresh if publisher metadata, correction, or retraction status changes.	PNAS DOI/publisher page and PubMed metadata verified live 2026-06-11; use for forecast-calibration claims.
[Ard, 2024]	Structured Analytic Techniques: A Pragmatic Approach	sat_evaluation_evidence	scholarly_peer_reviewed	2026-06-15	annual	Refresh if publisher metadata, correction, or retraction status changes.	DOI metadata verified live 2026-06-15 through Crossref for title, author, and publication year; publisher URL retained because automated publisher retrieval may be rate-limited.
[Jennifer Stromer-Galley and colleagues, 2020]	Flexible Versus Structured Support for Reasoning: Enhancing Analytical Reasoning Through a Flexible Analytic Technique	sat_evaluation_evidence	scholarly_repository	2026-06-11	annual	Refresh if repository metadata, DOI, or publisher record changes.	University of Glasgow repository metadata verified live 2026-06-11; use for flexible-SAT evidence as one bounded study, not all-purpose SAT proof.
[Betts, 1978]	Analysis, War, and Decision: Why Intelligence Failures Are Inevitable	intelligence_failures_postmortem	scholarly_peer_reviewed	2026-06-11	annual	Refresh if publisher metadata or DOI record changes.	Cambridge Core publisher page verified live 2026-06-11; use for failure-theory context, not fatalistic claims that improvement is impossible.
[Jervis, 2022]	Why Intelligence and Policymakers Clash	intelligence_failures_postmortem	scholarly_peer_reviewed	2026-06-11	annual	Refresh if publisher metadata, correction, or retraction status changes.	PNAS DOI/publisher metadata verified live 2026-06-11; use for postmortem and policy-friction boundary claims.
[Wirtz, 2023]	Are Intelligence Failures Still Inevitable?	intelligence_failures_postmortem	scholarly_peer_reviewed	2026-06-11	annual	Refresh if publisher metadata, correction, or retraction status changes.	DOI/publisher URL retained; scholarly metadata verified live 2026-06-11 from DOI-indexed search results because automated publisher retrieval was rate-limited.
[Central Intelligence Agency, 1993]	Words of Estimative Probability	analytic_uncertainty	official_primary	2026-06-14	annual	CIA source URL, release status, or public text materially changes	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Central Intelligence Agency, 1970s]	The IC's Struggle to Express Uncertainty in the 1970s	analytic_uncertainty	official_primary	2026-06-14	annual	CIA source URL, release status, or public text materially changes	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2018b]	Developing a Taxonomy of Intelligence Analysis Variables	analytic_method_design	official_primary	2026-06-14	annual	CIA source URL, release status, or public text materially changes	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Johnston, 2005]	Analytic Culture in the U.S. Intelligence Community	intelligence_profession	official_primary	2026-06-15	annual	CIA source URL, release status, or public text materially changes	Direct CIA CSI book page and static PDF URL verified on 2026-06-15; metadata updated to preserve the existing citation key while crediting the monograph author.
[Central Intelligence Agency, 1955]	The Need for an Intelligence Literature	intelligence_profession	official_primary	2026-06-14	annual	CIA source URL, release status, or public text materially changes	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2025b]	Studies in Intelligence Author's Guide 2025: Guidance Section Only	intelligence_writing	official_primary	2026-06-14	annual	CIA guide version, source URL, or public release status changes	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2025a]	Applying Epistemology to Intelligence Analysis	analytic_epistemology	official_primary	2026-06-14	annual	CIA source URL, release status, or public text materially changes	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2023]	Agile Analysis: Transforming Intelligence Production Through Lean Startup Principles	analytic_production	official_primary	2026-06-14	annual	CIA source URL, release status, or public text materially changes	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2018c]	Managing the Reliability Cycle: An Alternative Approach to Thinking About Intelligence Failure	intelligence_failure	official_primary	2026-06-14	annual	CIA source URL, release status, or public text materially changes	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2018f]	Why Bad Things Happen to Good Analysts	intelligence_failure	official_primary	2026-06-14	annual	CIA source URL, release status, or public text materially changes	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Central Intelligence Agency, 2019]	The Future of Analysis	ai_enabled_analysis	official_primary	2026-06-14	annual	CIA source URL, release status, or public text materially changes	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 1999]	Psychology of Intelligence Analysis	analytic_cognition_and_bias	official_primary	2026-06-14	annual	CIA source URL, release status, or public text materially changes	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov; note retains CIA disclaimer context.
[Central Intelligence Agency, 1994]	Sherman Kent and the Board of National Estimates: Collected Essays	declassified_analytic_history	official_primary	2026-06-14	annual	CIA source URL, release status, or public text materially changes	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2020]	Lessons from SABLE SPEAR: The Application of an Artificial Intelligence Methodology to Tactical Intelligence	ai_enabled_analysis	official_primary	2026-06-14	annual	CIA source URL, release status, or public text materially changes	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2018a]	A Call for More Humility in Intelligence Analysis	analytic_cognition_and_bias	official_primary	2026-06-14	annual	CIA source URL, release status, or public text materially changes	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2021a]	Voice of Experience: Principles of Intelligence Analysis	analytic_method_design	official_primary	2026-06-14	annual	CIA source URL, release status, or public text materially changes	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2018e]	War and Chance: Assessing Uncertainty in International Politics	analytic_uncertainty	official_primary	2026-06-14	annual	CIA source URL, release status, or public text materially changes	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2005a]	Fifty Years of Studies in Intelligence	intelligence_profession_and_tradecraft	official_primary	2026-06-14	annual	CIA source URL, release status, or public text materially changes	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2018d]	Thinking and Writing: Cognitive Science and Intelligence Analysis	intelligence_writing_and_review	official_primary	2026-06-14	annual	CIA source URL, release status, or public text materially changes	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Central Intelligence Agency, 2005b]	Creation of a National Institute for Analytic Methods	analytic_method_design	official_primary	2026-06-14	annual	CIA source URL, release status, or public text materially changes	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2006]	When Everything is Intelligence - Nothing is Intelligence	intelligence_professionalism	official_primary	2026-06-14	annual	CIA article URL, archive status, or public text materially changes	Direct URL verified on 2026-06-14 with curl HTTP 200 and text/html content from cia.gov.
[Central Intelligence Agency, 1998]	CIA and the Vietnam Policymakers: Three Episodes 1962-1968	declassified_analytic_history	official_primary	2026-06-14	annual	CIA source URL, release status, or public text materially changes	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2021b]	Intelligent Analysis: How to Defeat Uncertainty in High-Stakes Decisions	analytic_uncertainty_language	official_primary	2026-06-14	annual	CIA source URL, release status, or public text materially changes	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2017]	The Limits of Prediction - or, How I Learned to Stop Worrying About Black Swans and Love Analysis	forecasting_calibration_evidence	official_primary	2026-06-14	annual	CIA source URL, release status, or public text materially changes	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[Central Intelligence Agency, 2026]	Espionage in Our AI Future	ai_enabled_analysis_risk	official_primary	2026-06-14	annual	CIA source URL, release status, or public text materially changes	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.
[of the Director of National Intelligence, 2026a]	Annual Threat Assessment of the U.S. Intelligence Community 2026	current_threat_baseline	official_primary	2026-06-14	annual	new Annual Threat Assessment, source URL change, or report correction is released	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF title and content matched the Annual Threat Assessment.
[of the Director of National Intelligence, 2013a]	Intelligence Community Directive 205: Analytic Outreach	analytic_outreach_governance	official_primary	2026-06-14	annual	ODNI directive version, source URL, or policy text materially changes	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF title and text matched ICD 205 Analytic Outreach.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[of the Director of National Intelligence, 2008]	Intelligence Community Directive 207: National Intelligence Council	national_intelligence_council	official_government	primary	2026-06-14	annual	ODNI directive version, source URL, or policy text materially changes	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 207.
[of the Director of National Intelligence, 2017b]	Intelligence Community Directive 208: Maximizing the Utility of Analytic Products	analytic_product_dissemination	official_government	primary	2026-06-14	annual	ODNI directive version, source URL, or policy text materially changes	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 208.
[of the Director of National Intelligence, 2012]	Intelligence Community Directive 209: Tearline Production and Dissemination	tearlines_and_releasable_intelligence	official_government	primary	2026-06-14	annual	ODNI directive version, source URL, or policy text materially changes	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 209.
[of the Director of National Intelligence, 2013b]	Intelligence Community Directive 403: Foreign Disclosure and Release of Classified National Intelligence	foreign_disclosure_and_release	official_government	primary	2026-06-14	annual	ODNI directive version, source URL, or policy text materially changes	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 403.
[of the Director of National Intelligence, 2024a]	Intelligence Community Directive 405: Intelligence Diplomacy	intelligence_diplomacy	official_government	primary	2026-06-14	annual	ODNI directive version, source URL, or policy text materially changes	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 405.
[of the Director of National Intelligence, 2024b]	Intelligence Community Directive 406: IC Engagement with Non-State Entities	non_state_engagement	official_government	primary	2026-06-14	annual	ODNI directive version, source URL, or policy text materially changes	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 406.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[of the Director of National Intelligence, 2024c]	Intelligence Community Directive 503: Intelligence Community Information Environment Risk Management	ic_information_environment_risk	official_primary	2026-06-14	annual	ODNI directive version, source URL, or policy text materially changes	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 503.
[of the Director of National Intelligence, 2013f]	Intelligence Community Directive 900: Integrated Mission Management	integrated_mission_management	official_primary	2026-06-14	annual	ODNI directive version, source URL, or policy text materially changes	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 900.
[of the Director of National Intelligence, 2017a]	Intelligence Community Directive 121: Managing the Intelligence Community Information Environment	ic_information_environment_risk	official_primary	2026-06-14	annual	ODNI directive version, source URL, or policy text materially changes	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 121.
[of the Director of National Intelligence, 2022]	Intelligence Community Directive 211: IC Support to the CFIUS Threat Analysis Process	economic_security_review	official_primary	2026-06-14	annual	ODNI directive version, source URL, or policy text materially changes	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 211.
[of the Director of National Intelligence, 2013d]	Intelligence Community Directive 731: Supply Chain Risk Management	supply_chain_risk_management	official_primary	2026-06-14	annual	ODNI directive version, source URL, or policy text materially changes	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 731.
[of the Director of National Intelligence, 2013c]	Intelligence Community Directive 710: Classification and Control Markings System	classification_marking_governance	official_primary	2026-06-14	annual	ODNI directive version, source URL, or policy text materially changes	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 710.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[of the Director of National Intelligence, 2013e]	Intelligence Community Directive 750: Counterintelligence Programs	counterintelligence_oversight_governance	official__primary	2026-06-14	annual	ODNI directive version, source URL, or policy text materially changes	Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 750.
[Intelligence.gov, 2026e]	Mission	ic__public__transparency	official__primary	2026-06-14	quarterly	Intelligence.gov page content, URL, or public mission framing materially changes	Direct URL verified on 2026-06-14 through browser fetch because intelligence.gov returned 403 to plain curl; fetched HTML title and page content matched the mission page.
[Intelligence.gov, 2026b]	Our Values: Accountability	ic__public__transparency	official__primary	2026-06-14	quarterly	Intelligence.gov page content, URL, or public values framing materially changes	Direct URL verified on 2026-06-14 through browser fetch because intelligence.gov returned 403 to plain curl; fetched HTML title and page content matched the accountability page.
[Intelligence.gov, 2026f]	Our Values: Transparency	ic__public__transparency	official__primary	2026-06-14	quarterly	Intelligence.gov page content, URL, or public values framing materially changes	Direct URL verified on 2026-06-14 through browser fetch because intelligence.gov returned 403 to plain curl; fetched HTML title and page content matched the transparency page.
[Intelligence.gov, 2026a]	About This Site	ic__public__transparency	official__primary	2026-06-14	quarterly	Intelligence.gov page content, URL, or transparency-platform framing materially changes	Direct URL verified on 2026-06-14 through browser fetch because intelligence.gov returned 403 to plain curl; fetched HTML title and page content matched the About This Site page.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Intelligence.gov, 2026c]	Our Values: Collaboration	ic_public_transparency	official_primary	2026-06-14	quarterly	Intelligence.gov page content, URL, or public values framing materially changes	Direct URL verified on 2026-06-14 through browser fetch because intelligence.gov returned 403 to plain curl; fetched HTML title and page content matched the collaboration page.
[Intelligence.gov, 2026d]	Our Values: Innovation	ic_public_transparency	official_primary	2026-06-14	quarterly	Intelligence.gov page content, URL, or public values framing materially changes	Direct URL verified on 2026-06-14 through browser fetch because intelligence.gov returned 403 to plain curl; fetched HTML title and page content matched the innovation page.
[Agency, 2024b]	Defense OSINT Strategy 2024-2028	defense_osint_governance	official_primary	2026-06-14	annual	DIA strategy URL, public release version, or Defense OSINT policy text materially changes	Direct URL verified on 2026-06-14 through browser fetch because dia.mil returned 403 to plain curl; fetched PDF content matched the Defense OSINT Strategy.
[Agency, 2015]	DIA Style Manual for Intelligence Production	intelligence_writing_standards	official_primary	2026-06-14	annual	DIA FOIA URL, style manual version, or public release status changes	Direct URL verified on 2026-06-14 through browser fetch because dia.mil returned 403 to plain curl; fetched PDF metadata matched the DIA Style Manual.
[Agency, 2014]	DIA Instruction 5400.001: Privacy and Civil Liberties Program	rights_impact_privacy	official_primary	2026-06-14	annual	DIA instruction URL, release status, or public policy text materially changes	Direct URL verified on 2026-06-14 through browser fetch because dia.mil returned 403 to plain curl; fetched PDF content matched DIAI 5400.001.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Agency, 2026f]	NSA Cybersecurity Advisories and Guidance	cyber_defense_guidance_index	official_primary	2026-06-14	quarterly	NSA guidance index structure, source URL, or public guidance inventory materially changes	Direct URL verified on 2026-06-14 through browser fetch because nsa.gov returned 403 to plain curl; fetched HTML title and content matched the advisories and guidance page.
[Agency, 2026d]	About NSA Mission	ic_public_transparency	official_primary	2026-06-14	quarterly	NSA public mission page content or URL materially changes	Direct URL verified on 2026-06-14 through browser fetch because nsa.gov returned 403 to plain curl; fetched HTML title and content matched the NSA mission page.
[Agency, 2026e]	NSA Joins the ASD's ACSC and Others to Release Guidance on Agentic Artificial Intelligence Systems	agentic_ai_security_governance	official_primary	2026-06-14	quarterly	NSA press release, linked guidance, or public agentic AI adoption posture materially changes	Direct URL verified on 2026-06-14 through browser fetch because nsa.gov returned 403 to plain curl; fetched HTML title and content matched the agentic AI services release.
[Agency, 2017b]	GEOINT Basic Doctrine Publication 1	geoint_professional_doctrine	official_primary	2026-06-14	annual	NGA doctrine URL, publication version, or public doctrine text materially changes	Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from nga.mil.
[Agency, 2021]	NGA Releases New Data Strategy to Navigate Digital, GEOINT Revolution	geoint_data_governance	official_primary	2026-06-14	annual	NGA page content, data strategy version, or public URL materially changes	Direct URL verified on 2026-06-14 with curl HTTP 200 and text/html content from nga.mil.
[of Investigation, 2026]	Counterintelligence and Espionage	counterintelligence_program	official_primary	2026-06-14	quarterly	FBI page content, URL, or public counterintelligence mission framing materially changes	Direct URL verified on 2026-06-14 through browser search/open because fbi.gov returned 403 to plain curl; fetched content matched the Counterintelligence and Espionage page.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Office, 2026b]	About NRO History	declassified_reconnaissance_history	official_primary	2026-06-14	annual	NRO history page content, URL, or declassification-resource structure materially changes	Direct URL verified on 2026-06-14 through web search/open; official NRO page content matched the history and Center for the Study of National Reconnaissance description.
[Dylan and Stivang, 2025]	Emerging Technologies and National Security Intelligence	ai_enabled_analysis	scholarly_peer_reviewed	2026-06-15	annual	journal article, DOI landing page, or scholarly consensus about emerging-technology effects on intelligence work materially changes	Direct Taylor and Francis source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[Caballero and Jenkins, 2024]	On Large Language Models in National Security Applications	ai_enabled_analysis	scholarly_preprint	2026-06-15	semiannual	arXiv version, DOI record, national-security LLM literature, or risk framing materially changes	Direct arXiv source URL verified on 2026-06-15 with title, authors, abstract, DOI record, and subject metadata visible on the primary page.
[Mikhailov, 2023]	Optimizing National Security Strategies through LLM-Driven Artificial Intelligence Integration	ai_enabled_analysis	scholarly_preprint	2026-06-15	semiannual	arXiv version, related DOI, national-security AI literature, or claim scope materially changes	Direct arXiv source URL verified on 2026-06-15 with title, author, abstract, DOI metadata, and version history visible on the primary page.
[Revanth Gangi Reddy and Ji, 2023]	SmartBook: AI-Assisted Situation Report Generation for Intelligence Analysts	ai_enabled_analysis	scholarly_preprint	2026-06-15	semiannual	arXiv version, published venue metadata, evaluation claims, or analyst-support literature materially changes	Direct arXiv source URL verified on 2026-06-15 with title, authors, abstract, version metadata, and DOI record visible on the primary page.
[et al., 2024a]	Mind the Gap: Foundation Models and the Covert Proliferation of Military Intelligence, Surveillance, Target Acquisition, and Reconnaissance	ai_enabled_analysis	scholarly_preprint	2026-06-15	semiannual	arXiv version, military-AI risk literature, or foundation-model capability discussion materially changes	Direct arXiv HTML source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[et al., 2023a]	The Age of Synthetic Realities: Challenges and Opportunities	synthetic_media_provenance	preprint	2026-06-15	semiannual	arXiv version, synthetic-media detection literature, provenance standards, or misuse patterns materially changes	Direct arXiv source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2018]	The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation	ai_red_team_assurance	scholarly_report	2026-06-15	annual	AI misuse taxonomy, cited source URL, or consensus risk framing materially changes	Direct arXiv source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[for Security and Technology, 2022]	Adversarial Machine Learning and Cybersecurity	ai_red_team_assurance	public_domain_primary	2026-06-15	annual	CSET report URL, adversarial-ML taxonomy, cybersecurity guidance, or AI assurance practice materially changes	Direct CSET source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[Taddeo and Floridi, 2018]	Regulate Artificial Intelligence to Avert Cyber Arms Race	cyber_threat_intelligence	scholarly_commentary	2026-06-15	annual	Nature article URL, DOI metadata, or AI-cyber policy literature materially changes	Direct Nature article page was opened and verified on 2026-06-15 after the script fetch timed out; title, authors, date, and DOI were visible on the primary page.
[Project and Institute, 2024]	The Future of Intelligence Analysis: U.S.-Australia Project on AI and Human-Machine Teaming	ai_enabled_analysis	public_boundary	2026-06-15	annual	SCSP report URL, PDF, AI analytic-team recommendations, or public policy context materially changes	Direct SCSP report PDF was verified on 2026-06-15 through the current SCSP resource page after the attachment URL had moved.
[McMahon, 2024]	Analytic Tradecraft Standards in an Age of AI	analytic_tradecraft	public_domain_primary	2026-06-15	annual	Belfer report URL, PDF, DOI or citation metadata, or public analytic-tradecraft AI guidance materially changes	Direct Belfer report page and linked PDF were verified on 2026-06-15 after the attachment URL had moved; title, author, publication date, and report scope were visible.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[et al., 2019]	Analysis of Competing Hypotheses in Intelligence Analysis	sat_evaluation_evidence	scholarly_peer_review	2026-06-15	annual	Wiley article URL, DOI metadata, ACH evidence literature, or SAT evaluation consensus materially changes	Direct Wiley source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2024b]	Task Structure, Confirmation Bias, and the Generation of Alternative Hypotheses	sat_evaluation_evidence	scholarly_peer_review	2026-06-15	annual	SpringerOpen article URL, DOI metadata, task-structure literature, or confirmation-bias evidence materially changes	Direct SpringerOpen source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[The White House, 1988]	National Operations Security Program, NSDD 298	opsec_doctrine_governance	official_primary	2026-06-15	biennial	Reagan Library URL, public archive metadata, or official OPSEC historical-policy citation materially changes	Direct Reagan Library PDF source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[Wardle and Derakhshan, 2017]	Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making	cognitive_influence_security	public_domain_primary	2026-06-15	annual	Council of Europe PDF URL, information-disorder terminology, or platform-governance literature materially changes	Direct Council of Europe source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[Deng and UNIDIR, 2023]	Exploring Synthetic Data for Artificial Intelligence and Autonomous Systems: A Primer	model_data_provenance	public_domain_primary	2026-06-15	annual	UNIDIR report URL, PDF, synthetic-data governance literature, or autonomous-systems policy materially changes	Direct UNIDIR report page and PDF were verified on 2026-06-15 after the attachment URL had moved; title, author, citation, and scope were visible.
[for Strategic and Studies, 2022]	Crossing the Deepfake Rubicon	synthetic_media_provenance	public_domain_primary	2026-06-15	annual	CSIS page URL, synthetic-media policy landscape, or deepfake threat assessment materially changes	Direct CSIS source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[National Security Agency et al., 2023]	Contextualizing Deepfake Threats to Organizations	synthetic_media_provenance	official_primary	2026-06-15	semiannual	NSA/CISA/FBI deepfake guidance, PDF URL, or official synthetic-media threat framing materially changes	Direct defense.gov PDF source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[Agency, 2017a]	Active Social Engineering Defense	cyber_threat_intelligence	official_primary	2026-06-15	annual	DARPA program page, program status, public description, or defensive social-engineering literature materially changes	Direct DARPA source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2015]	Active Inference and Epistemic Value	cognitive_active_inference	scholarly_peer_review	2026-06-15	annual	PubMed record, DOI metadata, active-inference theory literature, or claim-scope interpretation materially changes	Direct PubMed source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2017]	Uncertainty, Epistemics and Active Inference	cognitive_active_inference	scholarly_peer_review	2026-06-15	annual	PMC record, DOI metadata, active-inference theory literature, or analogy caveats materially changes	Direct PMC source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2022]	A Step-by-Step Tutorial on Active Inference and Its Application to Empirical Data	cognitive_active_inference	scholarly_peer_review	2026-06-15	annual	PMC record, active-inference tutorial literature, implementation practice, or pedagogy materially changes	Direct PMC source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2021a]	Active Inference in Modeling Conflict	cognitive_active_inference	scholarly_preprint	2026-06-15	annual	Zenodo record, DOI metadata, active-inference conflict-modeling literature, or simulation caveats materially changes	DOI redirected to the Zenodo primary record with HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[Kozera, 2020]	Fitness OSINT: Identifying and Tracking Military and Security Personnel with Fitness Applications	osint_geoint	scholarly_peer_review	2026-06-15	annual	journal article URL, fitness-app privacy literature, OSINT leakage patterns, or platform practices materially changes	Direct journal source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[et al., 2025b]	Adversarial Machine Learning in Cybersecurity: A Review	ai_red_team_assurance	scholarly_peer_reviewed	2026-06-15	annual	journal article URL, adversarial-ML literature, AI security taxonomy, or defensive testing guidance materially changes	Direct journal source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2023b]	Challenges of Artificial Intelligence to Cognitive Security and Safety	cognitive_influence_security	scholarly_peer_reviewed	2026-06-15	annual	article URL, cognitive-security AI literature, or safety taxonomy materially changes	Direct journal PDF URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[Deppe and Schaal, 2024]	A Conceptual Framework and Method for a NATO ACT Concept for Cognitive Warfare	cognitive_influence_security	scholarly_peer_reviewed	2026-06-15	annual	PMC record, NATO cognitive-warfare concept literature, or terminology materially changes	Direct PMC source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[Terp and Breuer, 2022]	DISARM: A Framework for Analysis of Disinformation Campaigns	cognitive_influence_security	scholarly_peer_reviewed	2026-06-15	annual	IEEE record, DISARM framework version, influence-operation taxonomy, or defensive analysis practice materially changes	Direct IEEE source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2024c]	Large Language Models and Disinformation: A Double-Edged Sword	cognitive_influence_security	scholarly_peer_reviewed	2026-06-15	annual	IEEE record, LLM disinformation literature, detection methods, or policy guidance materially changes	Direct IEEE source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2025c]	Large Language Models Can Generate Election Disinformation	cognitive_influence_security	scholarly_peer_reviewed	2026-06-15	annual	PMC record, election-disinformation literature, LLM detection evidence, or policy context materially changes	Direct PMC source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2023c]	Fighting Fire with Fire: Using Large Language Models to Combat Disinformation	cognitive_influence_security	scholarly_peer_reviewed	2026-06-15	annual	ACL Anthology PDF, detection benchmark literature, LLM model changes, or method limitations materially changes	Direct ACL Anthology PDF URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Farid and Bohacek, 2022]	Protecting World Leaders Against Deep Fakes	synthetic_media_provenance	scholarly_peer_reviewed	2026-06-15	annual	PMC record, deepfake detection/protection literature, synthetic-media policy, or threat landscape materially changes	Direct PMC source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2020]	Human Cognition Through the Lens of Social Engineering Cyberattacks	cognitive_influence_security	scholarly_peer_reviewed	2026-06-15	annual	PMC record, social-engineering cognition literature, or cyber-awareness evidence materially changes	Direct PMC source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2021b]	Situation Awareness in Intelligence Scenarios	analytic_cognition_bias	scholarly_peer_reviewed	2026-06-15	annual	PMC record, situation-awareness literature, intelligence-training evidence, or claim scope materially changes	Direct PMC source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2024d]	AI Emergency Preparedness	agent_incident_response	scholarly_preprint	2026-06-15	semiannual	arXiv version, AI incident-preparedness literature, public-sector guidance, or risk taxonomy materially changes	Direct arXiv source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[et al., 2025a]	The AI Incident Regime	agent_incident_response	scholarly_preprint	2026-06-15	semiannual	arXiv version, AI incident reporting regimes, official policy changes, or scholarly governance literature materially changes	Direct arXiv HTML source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.
[Cooper, 2005]	Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis	analytic_tradecraft_evidence	official_primary	2026-06-15	annual	CIA CSI page, monograph URL, or public release status changes	Direct CIA CSI book page verified live 2026-06-15; used for analytic-culture reform context, not as proof that any specific SAT improves accuracy.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Janis, 1982]	Groupthink: Psychological Studies of Policy Decisions and Fiascoes	analytic_cognition_and_bias	scholarly_book_mediated	2026-06-15	annual	Bibliographic metadata, edition record, or accessible publisher record changes	Google Books bibliographic record verified live 2026-06-15 for title, author, edition, publisher, year, and ISBN metadata; used as bibliographic support because no current publisher landing page was available.
[Coulthart, 2016]	Why Do Analysts Use Structured Analytic Techniques? An In-depth Study of an American Intelligence Agency	sat_evaluation_evidence	scholarly_peer_reviewed	2026-06-15	annual	Publisher metadata, DOI record, correction, or retraction status changes	Crossref DOI metadata verified live 2026-06-15 for title, author, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.
[Coulthart, 2017]	An Evidence-Based Evaluation of 12 Core Structured Analytic Techniques	sat_evaluation_evidence	scholarly_peer_reviewed	2026-06-15	annual	Publisher metadata, DOI record, correction, or retraction status changes	Crossref DOI metadata verified live 2026-06-15 for title, author, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.
[Tetlock, 2018]	Restructuring Structured Analytic Techniques in Intelligence	sat_evaluation_evidence	scholarly_peer_reviewed	2026-06-15	annual	Publisher metadata, DOI record, correction, or retraction status changes	Crossref DOI metadata verified live 2026-06-15 for title, authors, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.
[Whitesmith, 2019]	The Efficacy of ACH in Mitigating Serial Position Effects and Confirmation Bias in an Intelligence Analysis Scenario	sat_evaluation_evidence	scholarly_peer_reviewed	2026-06-15	annual	Publisher metadata, DOI record, correction, or retraction status changes	Crossref DOI metadata verified live 2026-06-15 for title, author, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.
[Mandel, 2020]	Coherence of Probability Judgments from Uncertain Evidence: Does ACH Help?	sat_evaluation_evidence	scholarly_peer_reviewed_open	2026-06-15	annual	Publisher metadata, correction, or retraction status changes	Cambridge Core article page verified live 2026-06-15 for title, authors, journal record, and accessible article metadata.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Dhami, 2018]	Boosting Intelligence Analysts' Judgment Accuracy: What Works, What Fails?	forecasting_calibration_evidence	scholarly_peer_reviewed	2026-06-15	annual	Publisher metadata, correction, or retraction status changes	Cambridge Core article page verified live 2026-06-15 for title, authors, journal record, and accessible article metadata.
[Tetlock, 2015b]	Improving Intelligence Analysis With Decision Science	forecasting_calibration_evidence	scholarly_peer_reviewed	2026-06-15	annual	Publisher metadata, DOI record, correction, or retraction status changes	Crossref DOI metadata verified live 2026-06-15 for title, authors, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.
[Council, 2011]	Intelligence Analysis for Tomorrow: Advances from the Behavioral and Social Sciences	analytic_cognition_and_bias	scholarly_public_report	2026-06-15	annual	National Academies record, DOI metadata, edition, or access status changes	National Academies publisher record verified live 2026-06-15; Crossref DOI metadata for 10.17226/13040 verified title, publisher, and year.
[on Intelligence, 2004]	Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq	intelligence_failure_and_reform	official_primary	2026-06-15	biennial	Senate report URL, archival location, or official record status changes	Official Senate Intelligence Committee PDF URL verified live 2026-06-15 with successful redirect to current Senate-hosted PDF asset.
[Activity, 2010]	Aggregative Contingent Estimation	forecasting_calibration_evidence	official_primary	2026-06-15	annual	IARPA program page, solicitation status, related-publication links, or archived program metadata changes	Direct IARPA program page verified live 2026-06-15; used for program objectives and forecasting-evidence context, not as an AGEINT performance claim.
[Activity, 2023]	Rapid Explanation, Analysis and Sourcing Online	agentic_analytic_assistance	primary	2026-06-15	annual	IARPA program page, BAA status, technical description, or evaluation language changes	Direct IARPA program page verified live 2026-06-15; used for bounded analyst-assistance context and explicit non-replacement language.
[Helmer, 1963]	An Experimental Application of the DELPHI Method to the Use of Experts	forecasting_calibration_evidence	scholarly_peer_reviewed	2026-06-15	annual	Publisher metadata, DOI record, correction, or retraction status changes	Crossref DOI metadata verified live 2026-06-15 for title, authors, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Klein, 2007]	Performing a Project Premortem	analytic_method_pedagogy	professional_practice	2026-06-15	annual	Publisher page, author metadata, or access status changes	Harvard Business Review article page verified live 2026-06-15 for title, author, publication date, and publisher record.
[Marrin, 2012]	Improving Intelligence Analysis: Bridging the Gap between Scholarship and Practice	analytic_method_pedagogy	scholarly_book_monograph	2026-06-15	annual	Publisher metadata, DOI record, edition, or access status changes	Crossref DOI metadata verified live 2026-06-15 for title, author, publisher, and year; DOI URL retained as stable scholarly source.
[Svenmarck, 2021]	Overview of Structured Analytic Techniques for Assessment and Judgement of Major Events	analytic_method_pedagogy	official_research_report	2026-06-15	annual	FOI report page, report number, download link, or abstract metadata changes	FOI report-summary page verified live 2026-06-15 for title, author, report number FOI-R–5116–SE, date, abstract, and keywords.
[Service, 2021]	Technical Brief on Joint Structured Analysis Techniques	analytic_method_pedagogy	professional_practice_guidance	2026-06-15	annual	JIPS publication page, PDF, date, or guidance metadata changes	JIPS publication page verified live 2026-06-15 for title, authoring organization, date, purpose statement, and download link.
[Denzler, 2024]	Revisiting the Psychology of Structured Analytical Techniques	analytic_cognition_and_bias	scholarly_peer_review	2026-06-15	annual	Publisher metadata, DOI record, correction, or retraction status changes	Crossref DOI metadata verified live 2026-06-15 for title, author, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.
[Mandel, 2024]	Critical Review of the Analysis of Competing Hypotheses Technique: Lessons for the Intelligence Community	sat_evaluation_evidence	scholarly_peer_review	2026-06-15	annual	Publisher metadata, DOI record, correction, or retraction status changes	Crossref DOI metadata verified live 2026-06-15 for title, authors, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.
[Miksa, 2024]	Assessment Tabling: An Integrated Structured Analytic Technique for Improved Intelligence Analysis and Reasoning Visualisation	analytic_method_pedagogy	scholarly_peer_review	2026-06-15	annual	Publisher metadata, DOI record, correction, or retraction status changes	Crossref DOI metadata verified live 2026-06-15 for title, author, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Coulthart, 2025]	Structured Analytic Techniques in an Intelligence Fusion Centre: A Survey of Analyst Perspectives and Use	sat_evaluation_evidence	scholarly_peer_reviewed	2026-06-15	annual	Publisher metadata, DOI record, correction, or retraction status changes	Crossref DOI metadata verified live 2026-06-15 for title, authors, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.
[Gustafson, 2025]	Teaching Structured Analytic Techniques across Nations: Same, Same but Different	analytic_method_pedagogy	scholarly_peer_reviewed	2026-06-15	annual	Publisher metadata, DOI record, correction, or retraction status changes	Crossref DOI metadata verified live 2026-06-15 for title, authors, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.
[McCarthy, 2024]	Seeing the Futures: Evaluating the Application of Structured Analytic Technique Alternative Futures Analysis	warning_intelligence	scholarly_peer_reviewed_open	2026-06-15	annual	Journal page, DOI 10.36878/nsj20241103.08, PDF, correction, or access status changes	National Security Journal article page verified live 2026-06-15 for title, author, publication date, DOI, abstract, and PDF link.
[Ritchey, 2013]	General Morphological Analysis: A General Method for Non-Quantified Modelling	analytic_method_pedagogy	scholarly_methodology_note	2026-06-15	annual	Method page, PDF, revision note, or licensing statement changes	Swedish Morphological Society method page verified live 2026-06-15 for title, author, revision note, and method description; used as a public method source for Zwicky-derived morphological analysis.
[Pherson, 2014b]	Cases in Intelligence Analysis: Structured Analytic Techniques in Action	analytic_method_pedagogy	scholarly_textbook	2026-06-15	annual	Publisher page, edition, ISBN, or access status changes	SAGE College Publishing product page verified live 2026-06-15 for title, subtitle, authors, edition, publisher, date, ISBNs, and description.
[Pherson, 2020]	Critical Thinking for Strategic Intelligence	analytic_method_pedagogy	scholarly_textbook	2026-06-15	annual	Publisher page, edition, ISBN, or access status changes	SAGE College Publishing product page verified live 2026-06-15 for title, authors, third edition, publisher, date, ISBNs, and description.
[of the Army., 2006]	FM 2-22.3 Human Intelligence Collector Operations	humint_doctrine	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for humint_doctrine materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_army_fm_2_22_3_ retained.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[of the Director of National Intelligence., 2008]	ICD 304: Human Intelligence	humint_doctrine	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for humint_doctrine materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_odni_icd_304_humi retained.
[of the Director of National Intelligence., 2016]	ICD 310: Coordination of Clandestine Human Source Collection Outside the US	humint_doctrine	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for humint_doctrine materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_odni_icd_310_clanc retained.
[to Study Governmental Operations with Respect to Intelligence Activities, Church Committeea]	Church Committee Final Report Book I: Foreign and Military Intelligence (S. Rep. 94-755)	humint_oversight_history	public_domain_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for humint_oversight_history materially changes	Direct source URL reviewed on 2026-06-16; original proposal key public_church_committee_b retained.
[to Study Governmental Operations with Respect to Intelligence Activities, Church Committeeb]	Church Committee Book III: NSA Surveillance (S. Rep. 94-755)	sigint_oversight_history	public_domain_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for sigint_oversight_history materially changes	Direct source URL reviewed on 2026-06-16; original proposal key public_church_committee_b retained.
[of the Director of National Intelligence., 2007]	ICD 302: Document and Media Exploitation	humint_doctrine	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for humint_doctrine materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_odni_icd_302_dome retained.
[of the Joint Chiefs of Staff., 2012]	JP 2-01: Joint and National Intelligence Support to Military Operations (2012)	collection_management_doctrine	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for collection_management_doctrine materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_jcs_jp_2_01_intelligenc retained.
[Agency., n.d.]	TEMPEST: A Signal Problem (NSA Declassified)	sigint_emanations_intelligence	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for sigint_emanations_intelligence materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_nsa_tempest_signal retained.
[National Security Agency, Various years]	NSA Center for Cryptologic History: Historical Publications	sigint_history	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for sigint_history materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_nsa_center_cryptolo retained.
[of Standards and Technology., 2024a]	FIPS 203: ML-KEM Post-Quantum Key-Encapsulation Standard	cryptography_standards	official_primary	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for cryptography_standards materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_nist_fips_203_ml_k retained.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[of Standards and Technology., 2024b]	FIPS 204: ML-DSA Post-Quantum Digital Signature Standard	cryptography_standards	official_primary	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for cryptography_standards materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_nist_fips_204_ml_d retained.
[of Standards and Technology., 2024c]	FIPS 205: SLH-DSA Post-Quantum Hash-Based Signature Standard	cryptography_standards	official_primary	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for cryptography_standards materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_nist_fips_205_slh_d retained.
[Office of the Director of National Intelligence, 2022]	ODNI Declassified Report on Commercially Available Information (2022)	osint_doctrine	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for osint_doctrine materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_odni_cai_report_20 retained.
[of the Joint Chiefs of Staff., 2017]	JP 2-03: Geospatial Intelligence in Joint Operations (2017)	geoint_doctrine	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for geoint_doctrine materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_jp_2_03_geoint_joi retained.
[Clark, 2020]	Geospatial Intelligence: Origins and Evolution (Georgetown UP, 2020)	geoint_tradecraft	scholarly_book_monograph	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for geoint_tradecraft materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_clark_2020_geospat retained; stale or indirect proposal URL replaced with direct source record.
[Van Puyvelde, 2025]	The rise of open-source intelligence, EJIS 2025	osint_methodology	scholarly_repository_record	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for osint_methodology materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_van_puyvelde_2025 retained.
[of the Director of National Intelligence., Current]	ICD 206: Sourcing Requirements for Disseminated Analytic Products (with ICS 206-01 on PAI/CAI/OSINT)	osint_doctrine	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for osint_doctrine materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_odni_icd_206_sourc retained.
[Agency., 2018]	NGA Pub 1.0: GEOINT Basic Doctrine (2018)	geoint_doctrine	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for geoint_doctrine materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_nga_geoint_pub1_d retained.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[of the Director of National Intelligence., 2024]	ODNI Commercially Available Information Fact Sheet (May 2024)	osint_doctrine	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for osint_doctrine materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_odni_cai_fact_sheet retained.
[Hutchins, 2011]	Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains	cyber_threat_intelligence	professional_documentation	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for cyber_threat_intelligence materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_hutchins_2011_kill normalized to professional_hutchins_2011_ki
[Caltagirone, 2013]	The Diamond Model of Intrusion Analysis	cyber_threat_intelligence	professional_documentation	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for cyber_threat_intelligence materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_caltagirone_2013_d normalized to professional_caltagirone_2013_
[CISA, 2024]	PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure (AA24-038A)	apt_threat_intelligence	official_primary	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for apt_threat_intelligence materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_cisa_aa24_038a_vol retained.
[NSA, 2023]	PRC State-Sponsored Cyber Actor Living off the Land to Evade Detection (AA23-144A)	apt_threat_intelligence	official_primary	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for apt_threat_intelligence materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_cisa_aa23_144a_vol retained.
[DOE, 2022]	APT Cyber Tools Targeting ICS/SCADA Devices (AA22-103A)	apt_threat_intelligence	official_primary	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for apt_threat_intelligence materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_cisa_aa22_103a_ap retained.
[CISA., 2020]	Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations (AA20-352A)	supply_chain_intelligence	official_primary	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for supply_chain_intelligence materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_cisa_aa20_352a_sol retained.
[Lee, 2016]	Analysis of the Cyber Attack on the Ukrainian Power Grid	historical_ics_incidents	official_primary	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for historical_ics_incidents materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_eisac_sans_ukraine_ retained.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[for Cybersecurity, ENISA]	ENISA Threat Landscape 2024	cyber_threat_intelligence	official_primary	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for cyber_threat_intelligence materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_enisa_threat_landsc retained.
[Boyens, 2022]	Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (NIST SP 800-161 Rev. 1)	supply_chain_intelligence	official_primary	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for supply_chain_intelligence materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_nist_sp_800_161r1_ retained.
[Biden, 2021]	Executive Order 14028 on Improving the Nation's Cybersecurity	supply_chain_intelligence	official_primary	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for supply_chain_intelligence materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_whitehouse_eo_1402 retained; stale or indirect proposal URL replaced with direct source record.
[of Incident Response and Teams, FIRST]	Traffic Light Protocol (TLP) — FIRST Standards Definitions and Usage Guidance, Version 2.0	threat_intel_sharing	official_standards	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for threat_intel_sharing materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_first_tlp_v2 retained.
[Corporation, NERC]	NERC CIP Reliability Standards (CIP-002 through CIP-015)	ics_ot_security_standards	official_primary	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for ics_ot_security_standards materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_nerc_cip_standards retained.
[Cherepanov, 2017]	Win32/Industroyer: A New Threat for Industrial Control Systems	historical_ics_incidents	professional_documentation	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for historical_ics_incidents materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_eset_win32_industro normalized to professional_eset_win32_indus
[ICS-CERT., 2010]	ICSA-10-272-01: Stuxnet Malware Mitigation	historical_ics_incidents	official_primary	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for historical_ics_incidents materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_cisa_isc_cert_stuxn retained.
[CISA., 2022]	Control System Defense: Know the Opponent	ics_ot_security_standards	official_primary	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for ics_ot_security_standards materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_cisa_nsa_ics_know_ retained.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[ICS., 2017]	ICS Defense Use Case No. 6: Modular ICS Malware	historical_ics_incidents	official_primary	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for historical_ics_incidents materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_nerc_eisac_ukraine_ retained.
[for Network and Security, ENISA]	Protecting Industrial Control Systems: Recommendations for Europe and Member States	ics_ot_security_standards	official_primary	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for ics_ot_security_standards materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_enisa_protecting_ics retained; stale or indirect proposal URL replaced with direct source record.
[of Staff., 2012]	JP 3-13, Information Operations (2012)	information_operations_doctrine	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for information_operations_doctrine materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_dod_jp3_13_inform retained.
[of Staff., 2014b]	JP 3-13.2, Military Information Support Operations (2014)	psyop_miso_doctrine	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for psyop_miso_doctrine materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_dod_jp3_13_2_mis retained.
[Paul and Matthews., 2016]	The Russian "Firehose of Falsehood" Propaganda Model (RAND, 2016)	active_measures_disinformation	professional_documentation	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for active_measures_disinformation materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_paul_matthew normalized to professional_rand_paul_matth
[Lazer, 2018]	The science of fake news (Science, 2018)	disinformation_misinformation	scholarly_peer_review	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for disinformation_misinformation materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_lazer_2018_science_ retained.
[Network, FinCEN]	FinCEN SAR Narrative Guidance Package (2003/2006)	finint_sar_reporting	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for finint_sar_reporting materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_fincen_sar_narrative retained.
[of Financial Intelligence Units., 2023]	Egmont Group Principles for Information Exchange Between FIUs (April 2023)	finint_international_cooperation	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for finint_international_cooperation materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_egmont_group_fiu_ retained.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[on Drugs and Crime, UNODC]	UNODC Money Laundering, Proceeds of Crime and the Financing of Terrorism	finint_aml_cft_international	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for finint_aml_cft_international materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_unodc_money_laun retained.
[Schott, 2006]	World Bank/IMF Reference Guide to AML/CFT (2006)	finint_aml_cft_international	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for finint_aml_cft_international materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_worldbank_aml_refe retained.
[Counterintelligence and Center, NCSCb]	National Counterintelligence Strategy 2024 (NCSC/ODNI)	counterintelligence_strategy	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for counterintelligence_strategy materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_ncsc_national_ci_st retained.
[Counterintelligence and Center, NCSCa]	National Counterintelligence Strategy 2020–2022 (NCSC/ODNI)	counterintelligence_strategy	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for counterintelligence_strategy materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_ncsc_national_ci_st retained.
[Pennycook and Rand., 2021]	The psychology of fake news (Trends in Cognitive Sciences, 2021)	disinformation_cognitive_psychology	scholarly_peer_reviewed	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for disinformation_cognitive_psychology materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_pennycook_rand_20 retained.
[Starbird and Wilson., 2019]	Disinformation as Collaborative Work (ACM CSCW, 2019)	active_measures_information_operations	scholarly_peer_reviewed	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for active_measures_information_operations materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_starbird_wilson retained.
[Hoffman, 2007]	Conflict in the 21st Century: The Rise of Hybrid Wars (Potomac Institute, 2007)	hybrid_warfare_doctrine	scholarly_peer_reviewed	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for hybrid_warfare_doctrine materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_hoffman_2007_hybr retained.
[Mazarr, 2015]	Mastering the Gray Zone (USAWC Press, 2015)	gray_zone_competition_doctrine	scholarly_book_monograph	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for gray_zone_competition_doctrine materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_mazarr_2015_gray_ retained.
[of Defense., 2020]	Irregular Warfare Annex to the National Defense Strategy – Summary (DoD, 2020)	irregular_warfare_strategy	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for irregular_warfare_strategy materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_dod_iw_annex_202 retained.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[of Staff., 2014a]	JP 3-05, Special Operations (2014)	special_operations_doctrine	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for special_operations_doctrine_dod_jp3_05_special materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_dod_jp3_05_special retained.
[Cialdini, 1984]	Influence: The Psychology of Persuasion (Cialdini, 1984)	social_engineering_influence_psychology	scholarly_book_publication	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for social_engineering_influence_psychology materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_cialdini_1984_influence_psychology retained; stale or indirect proposal URL replaced with direct source record.
[of Excellence., 2021]	NATO StratCom COE Strategic Communications Hybrid Threats Toolkit (2021)	hybrid_warfare_stratcom	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for hybrid_warfare_stratcom materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_nato_stratcom_hybr retained.
[of Staff., 2013]	JP 2-0, Joint Intelligence (2013)	imint_joint_intelligence	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for imint_joint_intelligence materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_dod_jp2_0_joint_i retained.
[Pamment and Smith., 2022]	Attributing Information Influence Operations (NATO StratCom COE, 2022)	active_measures_attribution	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for active_measures_attribution materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_nato_stratcom_attr retained.
[Andrew, 1990]	KGB: The Inside Story	intelligence_history_soviet	scholarly_book_monograph	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for intelligence_history_soviet materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_andrew_gordievsky retained.
[Andrew, 1999]	The Sword and the Shield	intelligence_history_soviet	scholarly_book_monograph	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for intelligence_history_soviet materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_andrew_mitrokhin retained.
[Andrew, 2009]	The Defence of the Realm	intelligence_history_british	scholarly_book_monograph	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for intelligence_history_british materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_andrew_2009_defen retained.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Weiner, 2007]	Legacy of Ashes: The History of the CIA	intelligence_history_american	scholarly_book_monograph	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for intelligence_history_american materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_book_weiner_2007_legacy retained; stale or indirect proposal URL replaced with direct source record.
[to Study Governmental Operations with Respect to Intelligence Activities., 1976]	Church Committee Final Report (Internet Archive)	legal_oversight_intelligence	primary_source_public_domain	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for legal_oversight_intelligence materially changes	Direct source URL reviewed on 2026-06-16; original proposal key primary_source_public_domain_church_committee_19 retained.
[Tversky, 1974]	Judgment under Uncertainty: Heuristics and Biases	cognitive_bias_foundations	scholarly_repository_record	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for cognitive_bias_foundations materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_tversky_kahneman_ retained.
[Kahneman, 2011]	Thinking, Fast and Slow (Wikipedia)	cognitive_bias_foundations	scholarly_book_monograph	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for cognitive_bias_foundations materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_kahneman_2011_th retained; stale or indirect proposal URL replaced with direct source record.
[Lewandowsky, 2021]	Countering Misinformation through Inoculation and Prebunking	cognitive_security_inoculation	scholarly_peer_review	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for cognitive_security_inoculation materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_lewandowsky_vande retained.
[Lewandowsky, 2020]	The Debunking Handbook 2020	cognitive_security_inoculation	scholarly_repository_record	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for cognitive_security_inoculation materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_lewandowsky_cook_ retained.
[Pennycook, 2021]	Shifting Attention to Accuracy — Nature	cognitive_security_misinformation	scholarly_peer_review	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for cognitive_security_misinformation materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_pennycook_2021_ac retained.
[Tetlock, 2005]	Expert Political Judgment — Internet Archive	analytic_tradecraft_forecasting	scholarly_book_monograph	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for analytic_tradecraft_forecasting materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_tetlock_2005_exper retained.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Tetlock, 2015a]	Superforecasting — Google Play Books	analytic_tradecraft_forecasting	scholarly_book_mention	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for analytic_tradecraft_forecasting materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_tetlock_gardner_20 retained; stale or indirect proposal URL replaced with direct source record.
[Congress., 1978]	FISA 1978 — GovInfo (Statutes at Large)	legal_authorities_surveillance	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for legal_authorities_surveillance materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_fisa_1978_statute retained.
[Congress., 2001]	USA PATRIOT Act — GovInfo Compilation	legal_authorities_surveillance	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for legal_authorities_surveillance materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_usa_patriot_act_20 retained.
[Congress., 2015]	USA FREEDOM Act — GovInfo	legal_authorities_surveillance	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for legal_authorities_surveillance materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_usa_freedom_act_2 retained.
[Reagan, 1981]	EO 12333 — ODNI	legal_authorities_intelligence_collection	official_primary	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for legal_authorities_intelligence_collection materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_eo_12333_odni_tex retained; stale or indirect proposal URL replaced with direct source record.
[Quinlan, 2007]	Just Intelligence: Prolegomena — Semantic Scholar	ethics_of_intelligence	scholarly_repository_record	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for ethics_of_intelligence materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_quinlan_2007_just_ retained.
[Omand, 2010]	Securing the State — Google Books	ethics_of_intelligence	scholarly_book_mention	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for ethics_of_intelligence materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_omand_2010_securi retained.
[Omand, 2018]	Principled Spying — Georgetown University Press	ethics_of_intelligence	scholarly_book_mention	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for ethics_of_intelligence materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_omand_phythian_2 retained.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Russell, 2020]	Artificial Intelligence: A Modern Approach, 4th ed.	agent_foundations	scholarly_repository	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for agent_foundations materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_russell_norvig_2020 retained.
[Rao, 1995]	BDI Agents: From Theory to Practice	agent_foundations	scholarly_repository	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for agent_foundations materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_rao_georgeff_1995_ retained.
[Vaswani, 2017]	Attention Is All You Need	llm_architecture	scholarly_preprint	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for llm_architecture materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_vaswani_2017_atte retained.
[Yao, 2023b]	Tree of Thoughts: Deliberate Problem Solving with LLMs	agentic_reasoning	scholarly_preprint	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for agentic_reasoning materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_yao_2023_tree_of_ retained.
[Lewis, 2020]	Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks	agentic_memory	scholarly_preprint	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for agentic_memory materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_lewis_2020_rag retained.
[Patil, 2023]	Gorilla: Large Language Model Connected with Massive APIs	tool_use_agents	scholarly_preprint	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for tool_use_agents materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_patil_2023_gorilla retained.
[Qin, 2023]	ToolLLM: Facilitating Large Language Models to Master 16000+ Real-world APIs	tool_use_agents	scholarly_preprint	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for tool_use_agents materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_qin_2023_toolllm retained.
[Wu, 2023]	AutoGen: Enabling Next-Gen LLM Applications via Multi-Agent Conversation	multi_agent_frameworks	scholarly_preprint	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for multi_agent_frameworks materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_wu_2023_autogen retained.
[LangChain, 2025a]	LangChain Documentation	agentic_framework_docs	professional_documentation	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for agentic_framework_docs materially changes	Direct source URL reviewed on 2026-06-16; original proposal key professional_langchain_docume retained.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[LangChain, 2025b]	LangGraph Documentation	agentic_framework	professional_documentation	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for agentic_framework_dos materially changes	Direct source URL reviewed on 2026-06-16; original proposal key professional_langgraph_docum retained.
[CrewAI, 2025]	CrewAI Documentation	agentic_framework	professional_documentation	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for agentic_framework_dos materially changes	Direct source URL reviewed on 2026-06-16; original proposal key professional_crewai_documenta retained.
[Liang, 2022]	Holistic Evaluation of Language Models	llm_evaluation	scholarly_preprint	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for llm_evaluation materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_liang_2022_helm retained.
[Srivastava, 2022]	Beyond the Imitation Game: Quantifying and Extrapolating the Capabilities of LLMs	llm_evaluation	scholarly_preprint	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for llm_evaluation materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_srivastava_2022_big retained.
[Perez, 2022]	Ignore Previous Prompt: Attack Techniques For Language Models	adversarial_ai_security	scholarly_preprint	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for adversarial_ai_security materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_perez_2022_prompt retained.
[Ericsson, 1993]	The Role of Deliberate Practice in the Acquisition of Expert Performance	cognitive_performance	scholarly_repository	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for cognitive_performance materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_ericsson_1993_delib retained.
[Cepeda, 2006]	Distributed Practice in Verbal Recall Tasks	cognitive_performance	scholarly_repository	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for cognitive_performance materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_cepeda_2006_space retained.
[Walker, 2006]	Sleep, Memory, and Plasticity	cognitive_performance	scholarly_repository	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for cognitive_performance materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_walker_stickgold_20 retained.

Anchor	Source	Lane	Tier	Checked	Cadence	Refresh trigger	Verification note
[Kaplan, 1989]	The Experience of Nature: A Psychological Perspective	cognitive_performance	scholarly_book_metadata	2026-06-16	annual	source URL, source status, edition/version, or claim-scope boundary for cognitive_performance materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_kaplan_kaplan_198 retained; stale or indirect proposal URL replaced with direct source record.
[of Standards and Technology., 2024]	NIST IR 8547: Transition to Post-Quantum Cryptography Standards	cryptographic_standards	official_draft	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for cryptographic_standards materially changes	Direct source URL reviewed on 2026-06-16; original proposal key official_nist_pqc_migration retained.
[Weng, 2023]	LLM-powered Autonomous Agents	agentic_design_principles	professional_documentation	2026-06-16	semiannual	source URL, source status, edition/version, or claim-scope boundary for agentic_design_principles materially changes	Direct source URL reviewed on 2026-06-16; original proposal key scholarly_weng_2023_agent normalized to professional_weng_2023_agent

80.4 Citation workflow and source-section coverage

Section anchor. Section 80.
AGEINT citations are generated from source data, not patched into generated Markdown.

80.4.1 Contributor recipe

Section anchor. Section 80.

Source type	Primary edit surface	Key format	When to use
Source-guide reference	`data/curriculum/` and `data/curriculum/references/`	`ageintNNN`	A parsed guide source supports a curriculum title or section.
Curated research anchor	`data/research_anchors/` plus `src/intelligence_content/` routing	stable descriptive key	A directly verified official, standards, public-domain, or scholarly source supports generated synthesis.
Source-quality anchor	`src/manuscript_variables/` source-quality list	stable descriptive key	A baseline governance or source-quality standard applies across modules.

80.5 Add or extend a citation: preserve identity and record metadata

Section anchor. Section 80.

1. Preserve `ageint001` through `ageint231`; do not renumber locked source identities.
2. Append new source-guide references after the locked range. Current generated guide keys extend through `ageint312`.
3. For curated anchors, record `source_lane`, `source_tier`, `checked_as_of`, `verification_method`, `claim_scope`, `refresh_cadence`, `refresh_trigger`, `stakeholder_role`, `assurance_use`, and `rights_dimension`.
4. Use Pandoc citation syntax such as `[@ageint137]` or `[@official_nist_ai_rmf]`.
5. Use label-backed cross-references to the curriculum orientation section and curriculum-map figure rather than hard-coded section or figure numbers.
6. Rebuild from the AGEINT root:

```
uv run python scripts/build_curriculum.py
```

never hand-edit `output/manuscript/` as the source of truth.

80.5.1 Current citation coverage by source section

Coverage anchor. Parent appendix: Section 80. Citation coverage by source section is validated from the generated citation inventory.

Measure	Count
Source sections	723
Citation occurrences	1468
Unique source-guide keys	301
Zero-citation source sections	0
Distribution	1 citation(s): 275 section(s), 2 citation(s): 154 section(s), 3 citation(s): 291 section(s), 4 citation(s): 3 section(s)

80.5.2 Citation rows by source section

Section	Module and source section	Citations	Citation links
1.99	The Nature of Intelligence - V2 source-lane extension: bind The Nature of Intelligence to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[238, 2026]; [237, 2026]; [270, 2026]
1.101	The Nature of Intelligence - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for The Nature of Intelligence	3	[273, 2026]; [274, 2026]; [275, 2026]
1.102	The Nature of Intelligence - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for The Nature of Intelligence	3	[286, 2026]; [287, 2026]; [292, 2026]
1.1	The Nature of Intelligence - Defining Intelligence: Collection, Analysis, Production, Dissemination	3	[309, 2026]; [310, 2026]; [300, 2026]
1.2	The Nature of Intelligence - The Intelligence Cycle (Classic, Revised, and Critique)	2	[297, 2026]; [298, 2026]
1.3	The Nature of Intelligence - Types: Strategic, Operational, Tactical, Technical Intelligence	3	[309, 2026]; [310, 2026]; [300, 2026]
1.4	The Nature of Intelligence - Intelligence as Social and Epistemological Practice	1	[001, 2026]

Section	Module and source section	Citations	Citation links
1.5	The Nature of Intelligence - National, Corporate, and Private Intelligence: Structural Differences	2	[297, 2026]; [298, 2026]
1.6	The Nature of Intelligence - The Ethics of Intelligence: EO 12333, FISA, ICD 203, Allied Law	1	[002, 2026]
1.7	The Nature of Intelligence - Active Inference as a Unifying Cognitive Framework for Intelligence	1	[003, 2026]
1.8	The Nature of Intelligence - The AI Inflection Point: How Artificial Intelligence Reshapes Every Phase of the Intelligence Cycle	2	[004, 2026]; [005, 2026]
2.99	Intelligence Community Architectures - V2 source-lane extension: bind Intelligence Community Architectures to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[234, 2026]; [247, 2026]; [249, 2026]
2.101	Intelligence Community Architectures - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Intelligence Community Architectures	3	[276, 2026]; [277, 2026]; [284, 2026]
2.102	Intelligence Community Architectures - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Intelligence Community Architectures	3	[288, 2026]; [289, 2026]; [293, 2026]
2.1	Intelligence Community Architectures - U.S. Intelligence Community: 18 Agencies, Authorities, and Relationships	1	[006, 2026]
2.2	Intelligence Community Architectures - Soviet/Russian Architecture: Cheka → GPU → NKVD → MGB → KGB → SVR/FSB/GRU	2	[297, 2026]; [298, 2026]
2.3	Intelligence Community Architectures - British Architecture: MI5, MI6/SIS, GCHQ, DI, JIC	1	[007, 2026]
2.4	Intelligence Community Architectures - Israeli Architecture: Mossad, Shin Bet, Unit 8200, LAKAM	1	[008, 2026]
2.5	Intelligence Community Architectures - Chinese Architecture: MSS, PLA-SSF, United Front Work Department, APT Groups	1	[009, 2026]

Section	Module and source section	Citations	Citation links
2.6	Intelligence Community Architectures - Five Eyes and Allied Intelligence Sharing: BRUSA to UKUSA	2	[010, 2026]; [011, 2026]
2.7	Intelligence Community Architectures - Non-State Intelligence Actors: Terrorist, Criminal, PMC	1	[012, 2026]
2.8	Intelligence Community Architectures - Fusion Centers, JITFs, and Inter-Agency Coordination	2	[297, 2026]; [298, 2026]
2.9	Intelligence Community Architectures - Intelligence Oversight: Congressional, Judicial, Executive Mechanisms	2	[298, 2026]; [297, 2026]
3.99	Tradecraft: Core Principles - V2 source-lane extension: bind Tradecraft: Core Principles to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[237, 2026]; [266, 2026]; [269, 2026]
3.101	Tradecraft: Core Principles - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Tradecraft: Core Principles	3	[278, 2026]; [279, 2026]; [283, 2026]
3.102	Tradecraft: Core Principles - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Tradecraft: Core Principles	3	[290, 2026]; [291, 2026]; [294, 2026]
3.1	Tradecraft: Core Principles - What Is Tradecraft? Historical Definitions and Evolution	2	[013, 2026]; [014, 2026]
3.2	Tradecraft: Core Principles - Operational Security (OPSEC): Process and the Five-Step Method	2	[297, 2026]; [298, 2026]
3.3	Tradecraft: Core Principles - Compartmentation: Need-to-Know vs. Need-to-Share	2	[297, 2026]; [298, 2026]
3.4	Tradecraft: Core Principles - Cover: Official, Non-Official Cover (NOC), Deep Cover, Legends	1	[015, 2026]
3.5	Tradecraft: Core Principles - The Principle of Plausible Deniability	2	[297, 2026]; [298, 2026]
3.6	Tradecraft: Core Principles - Pattern-of-Life Analysis and How to Disrupt It	1	[016, 2026]
3.7	Tradecraft: Core Principles - Situational Awareness: Urban and Rural Tradecraft	1	[014, 2026]
3.8	Tradecraft: Core Principles - Code Words, Glossaries, and the Language of Espionage	1	[017, 2026]

Section	Module and source section	Citations	Citation links
3.9	Tradecraft: Core Principles - Return of Classical Tradecraft in the AI Era: Dead Drops, Brush Passes, In-Person Exchanges	3	[018, 2026]; [005, 2026]; [019, 2026]
4.99	Agent Recruitment - V2 source-lane extension: bind Agent Recruitment to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[238, 2026]; [239, 2026]; [240, 2026]
4.101	Agent Recruitment - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Agent Recruitment	3	[280, 2026]; [281, 2026]; [282, 2026]
4.102	Agent Recruitment - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Agent Recruitment	3	[292, 2026]; [295, 2026]; [296, 2026]
4.1	Agent Recruitment - The MICE Framework: Money, Ideology, Coercion/Compromise, Ego	2	[020, 2026]; [021, 2026]
4.2	Agent Recruitment - MICE Expanded: RASCLS — Reciprocity, Authority, Scarcity, Commitment, Liking, Social Proof	2	[298, 2026]; [297, 2026]
4.3	Agent Recruitment - Targeting, Spotting, and Initial Assessment	2	[020, 2026]; [021, 2026]
4.4	Agent Recruitment - Assessment and Development Operations	2	[020, 2026]; [021, 2026]
4.5	Agent Recruitment - The Recruitment Pitch: Methods and Psychology	1	[020, 2026]
4.6	Agent Recruitment - KGB Recruitment Doctrine: Psychological Methods and Manipulation	2	[021, 2026]; [022, 2026]
4.7	Agent Recruitment - Digital-Age Recruitment: LinkedIn, Telegram, Cryptocurrencies, Dark Web	1	[023, 2026]
4.8	Agent Recruitment - Shared Experience as a Recruitment Tool: Experimental Research	1	[024, 2026]
4.9	Agent Recruitment - How AI Lowers the Cost of Recruitment and Social Engineering	1	[004, 2026]
4.10	Agent Recruitment - Recruitment Ethics and Legal Constraints	2	[298, 2026]; [297, 2026]

Section	Module and source section	Citations	Citation links
5.99	Agent Handling and Management - V2 source-lane extension: bind Agent Handling and Management to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[239, 2026]; [240, 2026]; [241, 2026]
5.101	Agent Handling and Management - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Agent Handling and Management	3	[273, 2026]; [276, 2026]; [285, 2026]
5.102	Agent Handling and Management - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Agent Handling and Management	3	[286, 2026]; [290, 2026]; [294, 2026]
5.1	Agent Handling and Management - The Case Officer–Agent Relationship: Building, Maintaining, Testing Trust	1	[025, 2026]
5.2	Agent Handling and Management - Meeting Structures: Overt, Covert, and Clandestine	2	[029, 2026]; [004, 2026]
5.3	Agent Handling and Management - The Surveillance Detection Route (SDR)	2	[026, 2026]; [016, 2026]
5.4	Agent Handling and Management - Dead Drops: Physical and Digital Methods	2	[027, 2026]; [028, 2026]
5.5	Agent Handling and Management - Cutouts, Intermediaries, and Deniability Chains	1	[029, 2026]
5.6	Agent Handling and Management - Fronts and Shell Entities as Agent Infrastructure	1	[029, 2026]
5.7	Agent Handling and Management - Counter-Surveillance and Detecting Hostile Surveillance	2	[030, 2026]; [031, 2026]
5.8	Agent Handling and Management - Running Agents-in-Place: Frequency, Tasking, Validation	2	[029, 2026]; [004, 2026]
5.9	Agent Handling and Management - Burning, Exfiltrating, and Terminating Agents	2	[029, 2026]; [004, 2026]
5.10	Agent Handling and Management - KGB Working-with-Agents Doctrine (Declassified Manuals)	1	[032, 2026]

Section	Module and source section	Citations	Citation links
5.11	Agent Handling and Management - AI-Enhanced Micro-Expression Analysis for Source Validation	1	[004, 2026]
5.12	Agent Handling and Management - AI-Personalized Communication: Tailoring Persuasion to Source Personality	1	[004, 2026]
6.99	Source Protection and CI Integration - V2 source-lane extension: bind Source Protection and CI Integration to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[238, 2026]; [241, 2026]; [266, 2026]
6.101	Source Protection and CI Integration - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Source Protection and CI Integration	3	[274, 2026]; [278, 2026]; [280, 2026]
6.102	Source Protection and CI Integration - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Source Protection and CI Integration	3	[287, 2026]; [288, 2026]; [295, 2026]
6.1	Source Protection and CI Integration - Identifying Penetration: Signs of Compromise	3	[307, 2026]; [305, 2026]; [304, 2026]
6.2	Source Protection and CI Integration - Compartmentation in Agent Networks	1	[029, 2026]
6.3	Source Protection and CI Integration - Lie Detection, Vetting, Polygraph, and Its Alternatives	3	[307, 2026]; [305, 2026]; [304, 2026]
6.4	Source Protection and CI Integration - The Double-Agent Operation	1	[029, 2026]
6.5	Source Protection and CI Integration - Hostile Intelligence from Non-State Actors	1	[033, 2026]
6.6	Source Protection and CI Integration - Espionage in the AI Era: Why HUMINT Will Grow in Importance	2	[019, 2026]; [034, 2026]
7.99	SIGINT Fundamentals - V2 source-lane extension: bind SIGINT Fundamentals to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[255, 2026]; [258, 2026]; [261, 2026]

Section	Module and source section	Citations	Citation links
7.101	SIGINT Fundamentals - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for SIGINT Fundamentals	3	[279, 2026]; [282, 2026]; [284, 2026]
7.102	SIGINT Fundamentals - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for SIGINT Fundamentals	3	[289, 2026]; [291, 2026]; [296, 2026]
7.1	SIGINT Fundamentals - COMINT and ELINT: Definitions and Distinctions	1	[035, 2026]
7.2	SIGINT Fundamentals - Historical Foundations: WWII Axis SIGINT (NSA Declassified 9 Volumes)	1	[036, 2026]
7.3	SIGINT Fundamentals - Spartans in Darkness: SIGINT in the Indochina War, 1945–1975	1	[037, 2026]
7.4	SIGINT Fundamentals - CIA–NSA SIGINT Relationship, 1947–1970	2	[038, 2026]; [039, 2026]
7.5	SIGINT Fundamentals - NSA Basic Cryptography (Friedman Documents)	1	[040, 2026]
8.99	Modern SIGINT and Cryptography - V2 source-lane extension: bind Modern SIGINT and Cryptography to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[258, 2026]; [260, 2026]; [261, 2026]
8.101	Modern SIGINT and Cryptography - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Modern SIGINT and Cryptography	3	[275, 2026]; [276, 2026]; [283, 2026]
8.102	Modern SIGINT and Cryptography - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Modern SIGINT and Cryptography	3	[286, 2026]; [293, 2026]; [295, 2026]

Section	Module and source section	Citations	Citation links
8.1	Modern SIGINT and Cryptography - UKUSA and Five Eyes SIGINT Sharing	2	[041, 2026]; [042, 2026]
8.2	Modern SIGINT and Cryptography - Bulk Collection, Metadata Analysis, and Legal Frameworks	2	[298, 2026]; [297, 2026]
8.3	Modern SIGINT and Cryptography - The Cryptographic Arms Race: E2E Encryption and Lawful Access	2	[297, 2026]; [298, 2026]
8.4	Modern SIGINT and Cryptography - Covert Communications Tradecraft: OTPs, Burst Transmission, Digital Dead Drops	2	[027, 2026]; [028, 2026]
8.5	Modern SIGINT and Cryptography - Radio Frequency Intelligence (RFINT) and Technical Surveillance	2	[043, 2026]; [044, 2026]
8.6	Modern SIGINT and Cryptography - Technical Surveillance Countermeasures (TSCM): Threat Levels and Detection	2	[045, 2026]; [046, 2026]
8.7	Modern SIGINT and Cryptography - Non-Linear Junction Detectors, RF Spectrum Analysis, Infrared Imaging	3	[309, 2026]; [310, 2026]; [300, 2026]
8.8	Modern SIGINT and Cryptography - Steganography: LSB, DCT, and Network-Layer Methods	1	[028, 2026]
8.9	Modern SIGINT and Cryptography - Signal Authentication in the Deepfake Era	1	[018, 2026]
9.99	OSINT Foundations - V2 source-lane extension: bind OSINT Foundations to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[251, 2026]; [253, 2026]; [269, 2026]
9.101	OSINT Foundations - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for OSINT Foundations	3	[273, 2026]; [274, 2026]; [275, 2026]
9.102	OSINT Foundations - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for OSINT Foundations	3	[286, 2026]; [287, 2026]; [292, 2026]
9.1	OSINT Foundations - History and Rise of OSINT in the Intelligence Community	1	[047, 2026]
9.2	OSINT Foundations - IC OSINT Strategy 2024–2026	1	[048, 2026]

Section	Module and source section	Citations	Citation links
9.3	OSINT Foundations - OSINT vs. HUMINT vs. SIGINT: Comparative Value and Fusion	2	[301, 2026]; [298, 2026]
9.4	OSINT Foundations - Legal and Ethical Constraints in OSINT Collection	2	[298, 2026]; [297, 2026]
9.5	OSINT Foundations - OPSEC for OSINT Operators: The Sock Puppet Problem	2	[301, 2026]; [298, 2026]
9.6	OSINT Foundations - Open Source Intelligence: Trends and Issues	1	[049, 2026]
10.99	OSINT Techniques and Tools - V2 source-lane extension: bind OSINT Techniques and Tools to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[251, 2026]; [252, 2026]; [269, 2026]
10.101	OSINT Techniques and Tools - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for OSINT Techniques and Tools	3	[276, 2026]; [277, 2026]; [284, 2026]
10.102	OSINT Techniques and Tools - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for OSINT Techniques and Tools	3	[288, 2026]; [289, 2026]; [293, 2026]
10.1	OSINT Techniques and Tools - Search Engine Tradecraft: Google Dorking, Yandex, Bing, Shodan	2	[050, 2026]; [051, 2026]
10.2	OSINT Techniques and Tools - Social Media OSINT: Scraping, Graph Analysis, Identity Verification	2	[051, 2026]; [052, 2026]
10.3	OSINT Techniques and Tools - Maltego: Graph-Based OSINT Investigation	1	[051, 2026]
10.4	OSINT Techniques and Tools - Recon-ng: Python-Based Reconnaissance Framework	2	[052, 2026]; [053, 2026]
10.5	OSINT Techniques and Tools - SpiderFoot: Automated OSINT Collection	1	[052, 2026]
10.6	OSINT Techniques and Tools - FOCA, TheHarvester, Sherlock: Targeted Investigation Tools	1	[054, 2026]
10.7	OSINT Techniques and Tools - OSINT Framework (osintframework.com): Module Taxonomy	2	[051, 2026]; [052, 2026]
10.8	OSINT Techniques and Tools - Offline OSINT Environments: VM Architecture and Isolation	2	[051, 2026]; [052, 2026]
10.9	OSINT Techniques and Tools - IntelTechniques OSINT 11th Edition Methods and Workflows	2	[055, 2026]; [056, 2026]

Section	Module and source section	Citations	Citation links
11.99	GEOINT and Imagery Intelligence - V2 source-lane extension: bind GEOINT and Imagery Intelligence to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[253, 2026]; [255, 2026]; [270, 2026]
11.101	GEOINT and Imagery Intelligence - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for GEOINT and Imagery Intelligence	3	[278, 2026]; [279, 2026]; [283, 2026]
11.102	GEOINT and Imagery Intelligence - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for GEOINT and Imagery Intelligence	3	[290, 2026]; [291, 2026]; [294, 2026]
11.1	GEOINT and Imagery Intelligence - Geospatial Intelligence Fundamentals: IMINT, GEOINT, Mapping	1	[057, 2026]
11.2	GEOINT and Imagery Intelligence - GEOINT Essential Body of Knowledge (USGIF)	1	[058, 2026]
11.3	GEOINT and Imagery Intelligence - Commercial Satellite Platforms: Maxar, Planet, Sentinel-1/2	1	[059, 2026]
11.4	GEOINT and Imagery Intelligence - Change Detection and Pattern-of-Life Imagery Analysis	2	[302, 2026]; [297, 2026]
11.5	GEOINT and Imagery Intelligence - GEOINT in Counterinsurgency and Strike Operations	2	[302, 2026]; [297, 2026]
11.6	GEOINT and Imagery Intelligence - DoD GEOINT Accreditation and Training Standards	1	[060, 2026]
11.7	GEOINT and Imagery Intelligence - MCRP 2-10B.4: USMC GEOINT Manual	1	[057, 2026]
11.8	GEOINT and Imagery Intelligence - AI-Assisted Satellite Image Analysis: Object Detection and Chronolocation	2	[302, 2026]; [297, 2026]
11.9	GEOINT and Imagery Intelligence - Open-Source Geospatial Intelligence Library	1	[059, 2026]

Section	Module and source section	Citations	Citation links
12.99	Cyber Intelligence Fundamentals - V2 source-lane extension: bind Cyber Intelligence Fundamentals to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[258, 2026]; [261, 2026]; [266, 2026]
12.101	Cyber Intelligence Fundamentals - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Cyber Intelligence Fundamentals	3	[280, 2026]; [281, 2026]; [282, 2026]
12.102	Cyber Intelligence Fundamentals - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Cyber Intelligence Fundamentals	3	[292, 2026]; [295, 2026]; [296, 2026]
12.1	Cyber Intelligence Fundamentals - The Cyber Kill Chain (Lockheed Martin)	2	[061, 2026]; [062, 2026]
12.2	Cyber Intelligence Fundamentals - MITRE ATT&CK Framework: Enterprise Matrix v19	2	[063, 2026]; [064, 2026]
12.2.1	Cyber Intelligence Fundamentals - Reconnaissance through Resource Development	1	[063, 2026]
12.2.2	Cyber Intelligence Fundamentals - Initial Access, Execution, Persistence, Privilege Escalation	1	[065, 2026]
12.2.3	Cyber Intelligence Fundamentals - Defense Evasion, Credential Access, Discovery, Lateral Movement	3	[300, 2026]; [303, 2026]; [304, 2026]
12.2.4	Cyber Intelligence Fundamentals - Collection, Command & Control, Exfiltration, Impact	2	[062, 2026]; [063, 2026]
12.3	Cyber Intelligence Fundamentals - Unified Kill Chain: Extending Lockheed + MITRE	1	[062, 2026]
12.4	Cyber Intelligence Fundamentals - Threat Intelligence Sharing: STIX/TAXII Standards	3	[066, 2026]; [067, 2026]; [068, 2026]
12.5	Cyber Intelligence Fundamentals - Nation-State Cyber Espionage: Motivations and Methods	1	[069, 2026]
12.6	Cyber Intelligence Fundamentals - Chinese State-Affiliated Hacking: APT10, APT41, Volt Typhoon	2	[009, 2026]; [070, 2026]

Section	Module and source section	Citations	Citation links
12.7	Cyber Intelligence Fundamentals - Russian Cyber Operations: Sandworm, Cozy Bear, Fancy Bear	3	[300, 2026]; [303, 2026]; [304, 2026]
12.8	Cyber Intelligence Fundamentals - Living-Off-The-Land (LOTL) Techniques in APT Operations	1	[071, 2026]
13.99	Advanced Persistent Threats (APTs) - V2 source-lane extension: bind Advanced Persistent Threats (APTs) to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[237, 2026]; [258, 2026]; [261, 2026]
13.101	Advanced Persistent Threats (APTs) - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Advanced Persistent Threats (APTs)	3	[273, 2026]; [276, 2026]; [285, 2026]
13.102	Advanced Persistent Threats (APTs) - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Advanced Persistent Threats (APTs)	3	[286, 2026]; [290, 2026]; [294, 2026]
13.1	Advanced Persistent Threats (APTs) - APT Definitions, Lifecycle, and Attribution	1	[072, 2026]
13.2	Advanced Persistent Threats (APTs) - APT Risk Propagation Models: ATT&CK-Based Analysis	1	[072, 2026]
13.3	Advanced Persistent Threats (APTs) - Nation-State vs. Ideological Actor Attack Patterns	1	[069, 2026]
13.4	Advanced Persistent Threats (APTs) - APT Infrastructure: C2 Frameworks, Domain Fronting, Bulletproof Hosting	3	[300, 2026]; [303, 2026]; [304, 2026]
13.5	Advanced Persistent Threats (APTs) - Incident Response on Nation-State Intrusions: Mandiant Methodology	1	[071, 2026]
13.6	Advanced Persistent Threats (APTs) - Threat Hunting Against APT Actors	3	[300, 2026]; [303, 2026]; [304, 2026]
13.7	Advanced Persistent Threats (APTs) - APT Attribution: Technical Indicators vs. Geopolitical Context	3	[309, 2026]; [310, 2026]; [300, 2026]

Section	Module and source section	Citations	Citation links
14.99	Supply Chain Intelligence Attacks - V2 source-lane extension: bind Supply Chain Intelligence Attacks to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[258, 2026]; [266, 2026]; [268, 2026]
14.101	Supply Chain Intelligence Attacks - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Supply Chain Intelligence Attacks	3	[274, 2026]; [278, 2026]; [280, 2026]
14.102	Supply Chain Intelligence Attacks - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Supply Chain Intelligence Attacks	3	[287, 2026]; [288, 2026]; [295, 2026]
14.1	Supply Chain Intelligence Attacks - Supply Chain Operations as Strategic Intelligence Tradecraft	2	[297, 2026]; [298, 2026]
14.2	Supply Chain Intelligence Attacks - SolarWinds/SUNBURST: The Six-Month Patient Operation	1	[073, 2026]
14.3	Supply Chain Intelligence Attacks - XZ Utils/Jia Tan: Two-Year Social Engineering and Trust Infiltration	3	[074, 2026]; [075, 2026]; [076, 2026]
14.3.1	Supply Chain Intelligence Attacks - Sock Puppetry as HUMINT Cover Tradecraft	1	[076, 2026]
14.3.2	Supply Chain Intelligence Attacks - CVE-2024-3094: CVSS 10.0 Backdoor Mechanism	1	[076, 2026]
14.3.3	Supply Chain Intelligence Attacks - Attribution Indicators: APT29/SVR Pattern Similarities	1	[076, 2026]
14.3.4	Supply Chain Intelligence Attacks - “Friendly Yet Aggressive and Persistent” Social Engineering Signature	1	[076, 2026]
14.4	Supply Chain Intelligence Attacks - Open-Source Maintainer Targeting as an Acquisition Operation	1	[076, 2026]
14.5	Supply Chain Intelligence Attacks - Countermeasures: SBOM, SLSA Framework, Sigstore	3	[300, 2026]; [304, 2026]; [306, 2026]
14.6	Supply Chain Intelligence Attacks - Threat Intelligence Sharing for ICS Supply Chain (arXiv Survey)	1	[077, 2026]

Section	Module and source section	Citations	Citation links
15.99	Electronic and Emanations Intelligence - V2 source-lane extension: bind Electronic and Emanations Intelligence to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[255, 2026]; [256, 2026]; [261, 2026]
15.101	Electronic and Emanations Intelligence - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Electronic and Emanations Intelligence	3	[279, 2026]; [282, 2026]; [284, 2026]
15.102	Electronic and Emanations Intelligence - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Electronic and Emanations Intelligence	3	[289, 2026]; [291, 2026]; [296, 2026]
15.1	Electronic and Emanations Intelligence - ELINT: Radar Signatures and Weapons Systems Emissions	1	[035, 2026]
15.2	Electronic and Emanations Intelligence - EMINT: C4I System Emanations	1	[078, 2026]
15.3	Electronic and Emanations Intelligence - Tempest and Van Eck Radiation: Standards and Countermeasures	3	[300, 2026]; [303, 2026]; [304, 2026]
15.4	Electronic and Emanations Intelligence - Software-Defined Radio (SDR) for Intelligence Applications	3	[303, 2026]; [304, 2026]; [305, 2026]
15.5	Electronic and Emanations Intelligence - RF Mapping and Spectrum Intelligence	2	[302, 2026]; [297, 2026]
16.99	Imagery Intelligence (IMINT) - V2 source-lane extension: bind Imagery Intelligence (IMINT) to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[253, 2026]; [269, 2026]; [270, 2026]
16.101	Imagery Intelligence (IMINT) - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Imagery Intelligence (IMINT)	3	[275, 2026]; [276, 2026]; [283, 2026]

Section	Module and source section	Citations	Citation links
16.102	Imagery Intelligence (IMINT) - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Imagery Intelligence (IMINT)	3	[286, 2026]; [293, 2026]; [295, 2026]
16.1	Imagery Intelligence (IMINT) - Types: Optical, SAR, Infrared, Hyperspectral, Multispectral	2	[302, 2026]; [297, 2026]
16.2	Imagery Intelligence (IMINT) - Collection Platforms: Satellites, UAVs, Aircraft, Ground-Based	3	[309, 2026]; [310, 2026]; [300, 2026]
16.3	Imagery Intelligence (IMINT) - Photo Interpretation and All-Source Imagery Analysis	2	[302, 2026]; [297, 2026]
16.4	Imagery Intelligence (IMINT) - Commercial IMINT and the Democratization of Space-Based Reconnaissance	2	[302, 2026]; [297, 2026]
16.5	Imagery Intelligence (IMINT) - Open-Source Geolocation Methods: Bellingcat Methodology	2	[302, 2026]; [297, 2026]
17.99	Financial Intelligence (FININT) - V2 source-lane extension: bind Financial Intelligence (FININT) to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[251, 2026]; [252, 2026]; [254, 2026]
17.101	Financial Intelligence (FININT) - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Financial Intelligence (FININT)	3	[273, 2026]; [274, 2026]; [275, 2026]
17.102	Financial Intelligence (FININT) - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Financial Intelligence (FININT)	3	[286, 2026]; [287, 2026]; [292, 2026]
17.1	Financial Intelligence (FININT) - FININT Foundations: Collection, Analysis, Reporting	2	[079, 2026]; [080, 2026]
17.2	Financial Intelligence (FININT) - Suspicious Activity Reports (SARs) and Financial Intelligence Units	1	[079, 2026]
17.3	Financial Intelligence (FININT) - Terrorist Financing: Identification, Typologies, Interdiction	1	[079, 2026]

Section	Module and source section	Citations	Citation links
17.4	Financial Intelligence (FININT) - The SWIFT System and Intelligence Collection	1	[079, 2026]
17.5	Financial Intelligence (FININT) - Cryptocurrency as Covert Finance: Monero, Mixers, Bridges	2	[302, 2026]; [297, 2026]
17.6	Financial Intelligence (FININT) - Economic Warfare and FININT as a Strategic Tool	1	[081, 2026]
17.7	Financial Intelligence (FININT) - Money Laundering Detection: Data Mining and Matching Techniques	1	[080, 2026]
17.8	Financial Intelligence (FININT) - FININT Supporting National Security: Pillars and Methods	1	[082, 2026]
18.99	PSYOP and MISO Doctrine - V2 source-lane extension: bind PSYOP and MISO Doctrine to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[238, 2026]; [239, 2026]; [242, 2026]
18.101	PSYOP and MISO Doctrine - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for PSYOP and MISO Doctrine	3	[276, 2026]; [277, 2026]; [284, 2026]
18.102	PSYOP and MISO Doctrine - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for PSYOP and MISO Doctrine	3	[288, 2026]; [289, 2026]; [293, 2026]
18.1	PSYOP and MISO Doctrine - Joint PSYOP Doctrine: JP 3-53 (1996 and 2003)	2	[083, 2026]; [084, 2026]
18.2	PSYOP and MISO Doctrine - Military Information Support Operations (MISO): JP 3-13.2	1	[085, 2026]
18.3	PSYOP and MISO Doctrine - Tactical PSYOP TTP: FM 3-05.302	1	[086, 2026]
18.4	PSYOP and MISO Doctrine - FM 3-05.301: PSYOP Process Tactics and Techniques	1	[087, 2026]
18.5	PSYOP and MISO Doctrine - Target Audience Analysis (TAA) and Susceptibility Mapping	2	[302, 2026]; [297, 2026]
18.6	PSYOP and MISO Doctrine - PSYOP in Full-Spectrum Operations: Themes and Objectives	1	[086, 2026]
18.7	PSYOP and MISO Doctrine - Leaflets, Loudspeakers, and Digital Media: Product Development and Dissemination	2	[308, 2026]; [311, 2026]

Section	Module and source section	Citations	Citation links
19.99	Active Measures and Disinformation - V2 source-lane extension: bind Active Measures and Disinformation to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[238, 2026]; [239, 2026]; [240, 2026]
19.101	Active Measures and Disinformation - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Active Measures and Disinformation	3	[278, 2026]; [279, 2026]; [283, 2026]
19.102	Active Measures and Disinformation - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Active Measures and Disinformation	3	[290, 2026]; [291, 2026]; [294, 2026]
19.1	Active Measures and Disinformation - Soviet Active Measures: Definitions and Doctrine	2	[088, 2026]; [089, 2026]
19.2	Active Measures and Disinformation - Dezinformatsiya: Forgery, Front Organizations, Media Manipulation	2	[090, 2026]; [091, 2026]
19.3	Active Measures and Disinformation - KGB Aktivnyye Meropriyatiya: Historical Organization	1	[089, 2026]
19.4	Active Measures and Disinformation - Historical Active Measures Campaigns: INFEKTION, RYAN, DENVER	1	[091, 2026]
19.5	Active Measures and Disinformation - Russian Active Measures in the Contemporary Era	1	[092, 2026]
19.6	Active Measures and Disinformation - Chinese Information Operations: United Front Work Department	2	[308, 2026]; [311, 2026]
19.7	Active Measures and Disinformation - Deception, Disinformation, and Strategic Communications (NDU/Brown)	2	[093, 2026]; [094, 2026]
19.8	Active Measures and Disinformation - AI-Driven Active Measures: Synthetic Influence at Scale	2	[095, 2026]; [096, 2026]
19.9	Active Measures and Disinformation - Countermeasures: Disinformation Detection and Response	1	[092, 2026]

Section	Module and source section	Citations	Citation links
20.99	Social Engineering - V2 source-lane extension: bind Social Engineering to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[238, 2026]; [240, 2026]; [242, 2026]
20.101	Social Engineering - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Social Engineering	3	[280, 2026]; [281, 2026]; [282, 2026]
20.102	Social Engineering - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Social Engineering	3	[292, 2026]; [295, 2026]; [296, 2026]
20.1	Social Engineering - The Psychology of Influence: Cialdini's Seven Principles	1	[097, 2026]
20.2	Social Engineering - History of Social Engineering	1	[097, 2026]
20.3	Social Engineering - Social Engineering: The Science of Human Hacking (Hadnagy, 2018)	1	[098, 2026]
20.4	Social Engineering - The Art of Human Hacking (Hadnagy, 2010)	1	[099, 2026]
20.5	Social Engineering - Phishing, Vishing, Smishing, Deepfake Voice Attacks	3	[300, 2026]; [304, 2026]; [306, 2026]
20.6	Social Engineering - Physical Social Engineering: Access, Elicitation, Impersonation	2	[308, 2026]; [311, 2026]
20.7	Social Engineering - AI Automation of Social Engineering at Scale	1	[100, 2026]
20.8	Social Engineering - Defense: Training, Simulation, Technical Controls	2	[308, 2026]; [311, 2026]
21.99	Information Warfare and Cognitive Security - V2 source-lane extension: bind Information Warfare and Cognitive Security to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[238, 2026]; [239, 2026]; [244, 2026]
21.101	Information Warfare and Cognitive Security - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Information Warfare and Cognitive Security	3	[273, 2026]; [276, 2026]; [285, 2026]

Section	Module and source section	Citations	Citation links
21.102	Information Warfare and Cognitive Security - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Information Warfare and Cognitive Security	3	[286, 2026]; [290, 2026]; [294, 2026]
21.1	Information Warfare and Cognitive Security - Information Warfare Doctrine: Definitions, Theory, Air Force Policy	2	[101, 2026]; [102, 2026]
21.2	Information Warfare and Cognitive Security - Military Deception: Six Principles and Historical Effectiveness	2	[103, 2026]; [104, 2026]
21.3	Information Warfare and Cognitive Security - Automated Influence and the Cognitive Security Challenge	1	[105, 2026]
21.4	Information Warfare and Cognitive Security - Cognitive Security in the Age of AI: NATO/EU Paradigm Shift	1	[095, 2026]
21.5	Information Warfare and Cognitive Security - Epistemic Chaos as an Adversarial Goal	2	[095, 2026]; [096, 2026]
21.6	Information Warfare and Cognitive Security - Active Inference and Predictive Processing as Models for Cognitive Attack/Defense	2	[106, 2026]; [003, 2026]
21.7	Information Warfare and Cognitive Security - Behavioral Outcomes of Human Cognitive Security (arXiv 2026)	1	[107, 2026]
22.99	Counterintelligence Fundamentals - V2 source-lane extension: bind Counterintelligence Fundamentals to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[238, 2026]; [240, 2026]; [241, 2026]
22.101	Counterintelligence Fundamentals - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Counterintelligence Fundamentals	3	[274, 2026]; [278, 2026]; [280, 2026]

Section	Module and source section	Citations	Citation links
22.102	Counterintelligence Fundamentals - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Counterintelligence Fundamentals	3	[287, 2026]; [288, 2026]; [295, 2026]
22.1	Counterintelligence Fundamentals - CI Definition, Scope, Relationship to Intelligence	1	[012, 2026]
22.2	Counterintelligence Fundamentals - Offensive vs. Defensive Counterintelligence	1	[012, 2026]
22.3	Counterintelligence Fundamentals - Insider Threat Analysis: Critical Thinking Techniques (CDSE)	1	[108, 2026]
22.4	Counterintelligence Fundamentals - The Double-Agent and Triple-Cross Operations	2	[012, 2026]; [029, 2026]
22.5	Counterintelligence Fundamentals - Penetration of Hostile Services	2	[297, 2026]; [298, 2026]
22.6	Counterintelligence Fundamentals - Polygraph: Use and Limitations in CI	2	[297, 2026]; [298, 2026]
22.7	Counterintelligence Fundamentals - Damage Assessment and Control	2	[297, 2026]; [298, 2026]
22.8	Counterintelligence Fundamentals - Case Studies: Hanssen, Ames, Lee, Pollard	2	[297, 2026]; [298, 2026]
23.99	Counterintelligence Against Non-State Actors - V2 source-lane extension: bind Counterintelligence Against Non-State Actors to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[239, 2026]; [240, 2026]; [241, 2026]
23.101	Counterintelligence Against Non-State Actors - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Counterintelligence Against Non-State Actors	3	[279, 2026]; [282, 2026]; [284, 2026]
23.102	Counterintelligence Against Non-State Actors - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Counterintelligence Against Non-State Actors	3	[289, 2026]; [291, 2026]; [296, 2026]

Section	Module and source section	Citations	Citation links
23.1	Counterintelligence Against Non-State Actors - CI Against Terrorist and Criminal Intelligence Networks	1	[012, 2026]
23.2	Counterintelligence Against Non-State Actors - The Counterintelligence Threat from Non-State Actors	1	[033, 2026]
23.3	Counterintelligence Against Non-State Actors - CI in Hybrid Threat Environments	1	[109, 2026]
23.4	Counterintelligence Against Non-State Actors - Attribution Problems in Non-State CI Operations	1	[033, 2026]
23.5	Counterintelligence Against Non-State Actors - Corporate Counterintelligence and Trade Secret Protection	3	[307, 2026]; [305, 2026]; [304, 2026]
24.99	Gray Zone Warfare - V2 source-lane extension: bind Gray Zone Warfare to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[239, 2026]; [247, 2026]; [249, 2026]
24.101	Gray Zone Warfare - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Gray Zone Warfare	3	[275, 2026]; [276, 2026]; [283, 2026]
24.102	Gray Zone Warfare - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Gray Zone Warfare	3	[286, 2026]; [293, 2026]; [295, 2026]
24.1	Gray Zone Warfare - Defining the Gray Zone: Between Peace and War	2	[109, 2026]; [110, 2026]
24.2	Gray Zone Warfare - Gray Zone Tactics: Competition, Crisis, and Conflict	1	[111, 2026]
24.3	Gray Zone Warfare - Chinese Gray Zone: South China Sea and Taiwan Straits	2	[308, 2026]; [311, 2026]
24.4	Gray Zone Warfare - Russian Hybrid Warfare: Ukraine, Baltic States, Information Domain	1	[111, 2026]
24.5	Gray Zone Warfare - Anonymous No More: Countering Gray Zone Threats (MIPB 2025)	1	[111, 2026]
24.6	Gray Zone Warfare - Full Spectrum Conflict Design (IWI 2025)	1	[110, 2026]
25.99	Non-State Actor Intelligence - V2 source-lane extension: bind Non-State Actor Intelligence to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[238, 2026]; [247, 2026]; [249, 2026]

Section	Module and source section	Citations	Citation links
25.101	Non-State Actor Intelligence - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Non-State Actor Intelligence	3	[273, 2026]; [274, 2026]; [275, 2026]
25.102	Non-State Actor Intelligence - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Non-State Actor Intelligence	3	[286, 2026]; [287, 2026]; [292, 2026]
25.1	Non-State Actor Intelligence - Typology: Terrorist, Criminal, Commercial, Hacktivist, Proxy	1	[012, 2026]
25.2	Non-State Actor Intelligence - Hezbollah, ISIS, MS-13: Intelligence Structures and Capabilities	2	[308, 2026]; [311, 2026]
25.3	Non-State Actor Intelligence - Private Military Corporations as Intelligence Actors	2	[308, 2026]; [311, 2026]
25.4	Non-State Actor Intelligence - Counterintelligence Threat from Non-State Actors	1	[033, 2026]
25.5	Non-State Actor Intelligence - Non-State Actor Use of Commercial AI for Intelligence Collection	3	[309, 2026]; [310, 2026]; [300, 2026]
26.99	Irregular Warfare and Special Operations - V2 source-lane extension: bind Irregular Warfare and Special Operations to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[239, 2026]; [249, 2026]; [266, 2026]
26.101	Irregular Warfare and Special Operations - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Irregular Warfare and Special Operations	3	[276, 2026]; [277, 2026]; [284, 2026]
26.102	Irregular Warfare and Special Operations - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Irregular Warfare and Special Operations	3	[288, 2026]; [289, 2026]; [293, 2026]

Section	Module and source section	Citations	Citation links
26.1	Irregular Warfare and Special Operations - SF Unconventional Warfare Doctrine: TC 18-01	1	[112, 2026]
26.2	Irregular Warfare and Special Operations - FM 3-05.130: ARSOF Unconventional Warfare	2	[113, 2026]; [114, 2026]
26.3	Irregular Warfare and Special Operations - FM 3-05.102: ARSOF Intelligence	2	[115, 2026]; [116, 2026]
26.4	Irregular Warfare and Special Operations - OSS Origins and Training Manuals (1944)	3	[117, 2026]; [118, 2026]; [119, 2026]
26.5	Irregular Warfare and Special Operations - Principles of Tradecraft for Resistance Organizations	1	[120, 2026]
26.6	Irregular Warfare and Special Operations - Underground Intelligence Networks: Structure, Security, Continuity	2	[308, 2026]; [311, 2026]
26.7	Irregular Warfare and Special Operations - OSS Simple Sabotage Field Manual (1944)	1	[117, 2026]
26.8	Irregular Warfare and Special Operations - Morale Operations: OSS Psychological Warfare	1	[117, 2026]
27.99	Soviet and Russian Intelligence - V2 source-lane extension: bind Soviet and Russian Intelligence to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[266, 2026]; [267, 2026]; [269, 2026]
27.101	Soviet and Russian Intelligence - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Soviet and Russian Intelligence	3	[278, 2026]; [279, 2026]; [283, 2026]
27.102	Soviet and Russian Intelligence - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Soviet and Russian Intelligence	3	[290, 2026]; [291, 2026]; [294, 2026]
27.1	Soviet and Russian Intelligence - KGB Structure, Culture, and Doctrine: First Chief Directorate	1	[121, 2026]
27.2	Soviet and Russian Intelligence - The Lubyanka Files: 29 KGB Training Manuals, 1965–1989	1	[122, 2026]
27.2.1	Soviet and Russian Intelligence - Working with Agents (Declassified Manual)	1	[032, 2026]

Section	Module and source section	Citations	Citation links
27.2.2	Soviet and Russian Intelligence - Working with Information in Intelligence (1970s)	1	[121, 2026]
27.2.3	Soviet and Russian Intelligence - Psychological Methods and Manipulation of Agents (1988)	1	[021, 2026]
27.2.4	Soviet and Russian Intelligence - Some Aspects of Training Agents Psychologically (1985)	1	[021, 2026]
27.2.5	Soviet and Russian Intelligence - Exposure of Disinformation in Intelligence Materials (1968)	1	[021, 2026]
27.2.6	Soviet and Russian Intelligence - Organizational Structure and Management of Intelligence Residency	2	[297, 2026]; [298, 2026]
27.2.7	Soviet and Russian Intelligence - On Organizing Work with Confidential Contacts	1	[122, 2026]
27.2.8	Soviet and Russian Intelligence - Tasks of a KGB Resident Abroad	1	[122, 2026]
27.3	Soviet and Russian Intelligence - KGB Alpha Team Training Manual	1	[123, 2026]
27.4	Soviet and Russian Intelligence - The Mitrokhin Archive: KGB Global Operations	4	[124, 2026]; [125, 2026]; [126, 2026]; [127, 2026]
27.5	Soviet and Russian Intelligence - GRU: Soviet Military Intelligence Structure	2	[297, 2026]; [298, 2026]
27.6	Soviet and Russian Intelligence - The Interpreter Magazine: KGB Manual Summaries	1	[022, 2026]
28.99	American Intelligence History - V2 source-lane extension: bind American Intelligence History to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[266, 2026]; [269, 2026]; [271, 2026]
28.101	American Intelligence History - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for American Intelligence History	3	[280, 2026]; [281, 2026]; [282, 2026]
28.102	American Intelligence History - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for American Intelligence History	3	[292, 2026]; [295, 2026]; [296, 2026]
28.1	American Intelligence History - OSS in World War II	2	[128, 2026]; [129, 2026]
28.1.1	American Intelligence History - OSS Secret Intelligence Manual	1	[117, 2026]

Section	Module and source section	Citations	Citation links
28.1.2	American Intelligence History - OSS Provisional Basic Field Manual	1	[119, 2026]
28.1.3	American Intelligence History - Special Operations Field Manual	1	[118, 2026]
28.1.4	American Intelligence History - OSS Special Weapons and Devices	1	[117, 2026]
28.1.5	American Intelligence History - Simple Sabotage Field Manual (1944)	1	[117, 2026]
28.1.6	American Intelligence History - Morale Operations Field Manual	1	[117, 2026]
28.2	American Intelligence History - CIA Cold War Operations	2	[297, 2026]; [298, 2026]
28.2.1	American Intelligence History - CIA Manual of Trickery and Deception (Mulholland)	1	[130, 2026]
28.2.2	American Intelligence History - Principles of Tradecraft (Resistance Operations)	1	[120, 2026]
28.2.3	American Intelligence History - Soviet Active Measures Documents (CREST Collection)	4	[088, 2026]; [089, 2026]; [090, 2026]; [091, 2026]
28.3	American Intelligence History - Studies in Intelligence: The CIA's Professional Journal	3	[131, 2026]; [132, 2026]; [133, 2026]
28.3.1	American Intelligence History - Vol. 70, No. 1 (March 2026): "Espionage in Our AI Future" (Mulligan/RAND)	2	[019, 2026]; [034, 2026]
28.3.2	American Intelligence History - Vol. 68, No. 2 (June 2024): OSINT in the IC	1	[047, 2026]
28.4	American Intelligence History - History of SIGINT at the CIA, 1947–1970	2	[038, 2026]; [039, 2026]
28.5	American Intelligence History - NSA WWII Declassified: European Axis SIGINT (9 Volumes)	1	[036, 2026]
29.99	British and Allied Intelligence - V2 source-lane extension: bind British and Allied Intelligence to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[266, 2026]; [269, 2026]; [270, 2026]
29.101	British and Allied Intelligence - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for British and Allied Intelligence	3	[273, 2026]; [276, 2026]; [285, 2026]
29.102	British and Allied Intelligence - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for British and Allied Intelligence	3	[286, 2026]; [290, 2026]; [294, 2026]
29.1	British and Allied Intelligence - MI6/SIS: Structure and Cold War Tradecraft	1	[007, 2026]

Section	Module and source section	Citations	Citation links
29.2	British and Allied Intelligence - SOE: Special Operations Executive Training (WWII)	1	[134, 2026]
29.3	British and Allied Intelligence - GCHQ and the BRUSA/UKUSA Agreements	2	[011, 2026]; [135, 2026]
29.4	British and Allied Intelligence - Five Eyes Archive: Key Declassified Documents	3	[010, 2026]; [041, 2026]; [042, 2026]
30.99	Israeli and Continental Services - V2 source-lane extension: bind Israeli and Continental Services to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[266, 2026]; [267, 2026]; [271, 2026]
30.101	Israeli and Continental Services - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Israeli and Continental Services	3	[274, 2026]; [278, 2026]; [280, 2026]
30.102	Israeli and Continental Services - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Israeli and Continental Services	3	[287, 2026]; [288, 2026]; [295, 2026]
30.1	Israeli and Continental Services - Mossad: Structure, Culture, Notable Operations	1	[008, 2026]
30.2	Israeli and Continental Services - Eli Cohen: Deep Cover Agent in Syria	1	[136, 2026]
30.3	Israeli and Continental Services - Operation Wrath of God: PSYOP and Targeted Killing	2	[297, 2026]; [298, 2026]
30.4	Israeli and Continental Services - Unit 8200: SIGINT, AI, and Cyber Excellence	2	[297, 2026]; [298, 2026]
30.5	Israeli and Continental Services - SDECE/DGSE: French Intelligence Tradition	2	[297, 2026]; [298, 2026]
30.6	Israeli and Continental Services - BND: German Federal Intelligence Service	2	[297, 2026]; [298, 2026]
30.7	Israeli and Continental Services - Stasi: East German Pervasive Domestic Intelligence	2	[297, 2026]; [298, 2026]
31.99	Foundations of AGEINT - V2 source-lane extension: bind Foundations of AGEINT to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[232, 2026]; [235, 2026]; [247, 2026]

Section	Module and source section	Citations	Citation links
31.100	Foundations of AGEINT - V2 AGEINT-depth extension: add agent evaluation and public-sector adoption gates that bind agency authority, AI Office-style accountability, impact assessment, and human review before any classroom agent workflow is rehearsed	3	[232, 2026]; [235, 2026]; [247, 2026]
31.101	Foundations of AGEINT - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Foundations of AGEINT	3	[279, 2026]; [282, 2026]; [284, 2026]
31.102	Foundations of AGEINT - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Foundations of AGEINT	3	[289, 2026]; [291, 2026]; [296, 2026]
31.1	Foundations of AGEINT - Defining AGEINT: From AI Agents to Autonomous Intelligence Systems	3	[299, 2026]; [306, 2026]; [312, 2026]
31.2	Foundations of AGEINT - From LLMs to Agents: The Cognitive Controller Stack	1	[137, 2026]
31.3	Foundations of AGEINT - Unified Taxonomy: Perception → Brain → Planning → Action → Collaboration	1	[137, 2026]
31.3.1	Foundations of AGEINT - Perception Modules: Multimodal Ingestion (Text, Vision, Audio, Sensor)	3	[299, 2026]; [306, 2026]; [312, 2026]
31.3.2	Foundations of AGEINT - Brain/Reasoning: LLM as Cognitive Controller	1	[138, 2026]
31.3.3	Foundations of AGEINT - Memory: In-Context, External VectorDB, Episodic, Semantic, Procedural	3	[299, 2026]; [306, 2026]; [312, 2026]
31.3.4	Foundations of AGEINT - Action: Tool Use, API Calls, Code Execution, Computer Use	3	[299, 2026]; [306, 2026]; [312, 2026]
31.3.5	Foundations of AGEINT - Collaboration: A2A Messaging, Shared Context, Role Specialization	1	[139, 2026]
31.4	Foundations of AGEINT - The OECD Agentic AI Landscape and Conceptual Foundations (2026)	1	[140, 2026]
31.5	Foundations of AGEINT - MIT Sloan Explanation of Agentic AI	1	[141, 2026]
31.6	Foundations of AGEINT - AGEINT vs. Traditional OSINT vs. AI-Assisted Analysis: A Capability Matrix	2	[301, 2026]; [298, 2026]
31.7	Foundations of AGEINT - Dual-Paradigm Framework: Symbolic/Classical vs. Neural/Generative Agents	1	[142, 2026]

Section	Module and source section	Citations	Citation links
31.8	Foundations of AGEINT - The Return to HUMINT as Agentic AI Degrades Digital Trust	2	[004, 2026]; [005, 2026]
32.99	AGEINT Design Patterns and Archetypes - V2 source-lane extension: bind AGEINT Design Patterns and Archetypes to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[233, 2026]; [258, 2026]; [272, 2026]
32.100	AGEINT Design Patterns and Archetypes - V2 AGEINT-depth extension: transform every raw design motif into a safe registry entry, tabletop audit, provenance record, and interface contract rather than operational deployment	3	[233, 2026]; [258, 2026]; [272, 2026]
32.101	AGEINT Design Patterns and Archetypes - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for AGEINT Design Patterns and Archetypes	3	[275, 2026]; [276, 2026]; [283, 2026]
32.102	AGEINT Design Patterns and Archetypes - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for AGEINT Design Patterns and Archetypes	3	[286, 2026]; [293, 2026]; [295, 2026]
module section	AGEINT Design Patterns and Archetypes - Pattern 1: The Solo Reasoner — Single-agent ReAct loop for focused intelligence tasks	1	[143, 2026]
module section	AGEINT Design Patterns and Archetypes - Methods: Chain-of-Thought, Self-Critique, Reflection Scoring	3	[309, 2026]; [310, 2026]; [300, 2026]
module section	AGEINT Design Patterns and Archetypes - Application: Single-source report analysis, indicator enrichment	3	[309, 2026]; [310, 2026]; [300, 2026]
module section	AGEINT Design Patterns and Archetypes - Code Archetype: LangChain LCEL ReAct agent with tool calling	3	[299, 2026]; [306, 2026]; [312, 2026]
module section	AGEINT Design Patterns and Archetypes - Pattern 2: The Reflection Agent — Self-evaluation after each action step	1	[139, 2026]
module section	AGEINT Design Patterns and Archetypes - Methods: Internal scoring, critic models, trajectory validation	2	[306, 2026]; [312, 2026]

Section	Module and source section	Citations	Citation links
module section	AGEINT Design Patterns and Archetypes - Application: OSINT verification loop, analytic bias detection	2	[297, 2026]; [298, 2026]
module section	AGEINT Design Patterns and Archetypes - Code Archetype: LangGraph state machine with reflexion node	3	[299, 2026]; [306, 2026]; [312, 2026]
module section	AGEINT Design Patterns and Archetypes - Pattern 3: The Tool-Forager — Agent with comprehensive external tool access	1	[144, 2026]
module section	AGEINT Design Patterns and Archetypes - Methods: Function calling, JSON schema execution, grounded output	3	[309, 2026]; [310, 2026]; [300, 2026]
module section	AGEINT Design Patterns and Archetypes - Application: Multi-source data harvesting, real-time collection	3	[309, 2026]; [310, 2026]; [300, 2026]
module section	AGEINT Design Patterns and Archetypes - Code Archetype: OpenAI function calling with Recon-ng, Shodan, STIX tools	3	[309, 2026]; [310, 2026]; [300, 2026]
module section	AGEINT Design Patterns and Archetypes - Pattern 4: The Planner-Executor — Long-horizon task decomposition	2	[139, 2026]; [145, 2026]
module section	AGEINT Design Patterns and Archetypes - Methods: Chain-of-thought with memory rehydration, execution DAGs	3	[299, 2026]; [306, 2026]; [312, 2026]
module section	AGEINT Design Patterns and Archetypes - Application: Multi-phase operation planning, collection management	3	[309, 2026]; [310, 2026]; [300, 2026]
module section	AGEINT Design Patterns and Archetypes - Code Archetype: LangGraph DAG flow with priority queues	3	[299, 2026]; [306, 2026]; [312, 2026]
module section	AGEINT Design Patterns and Archetypes - Pattern 5: The Parallel Collector — Concurrent multi-source collection	1	[144, 2026]
module section	AGEINT Design Patterns and Archetypes - Methods: Concurrent tool invocation, aggregation, deduplication	3	[299, 2026]; [306, 2026]; [312, 2026]
module section	AGEINT Design Patterns and Archetypes - Application: Simultaneous OSINT/SIGINT metadata collection	2	[301, 2026]; [298, 2026]
module section	AGEINT Design Patterns and Archetypes - Code Archetype: CrewAI parallel task execution with consensus scoring	3	[299, 2026]; [306, 2026]; [312, 2026]
module section	AGEINT Design Patterns and Archetypes - Pattern 6: The Multi-Agent Crew — Specialized agents in collaborative formation	2	[139, 2026]; [146, 2026]
module section	AGEINT Design Patterns and Archetypes - Methods: Planner + Retriever + Executor + Validator + Reporter roles	3	[299, 2026]; [306, 2026]; [312, 2026]
module section	AGEINT Design Patterns and Archetypes - Application: All-source intelligence fusion; Red/Blue Cell simulation	3	[299, 2026]; [306, 2026]; [312, 2026]

Section	Module and source section	Citations	Citation links
module section	AGEINT Design Patterns and Archetypes - Code Archetype: CrewAI role-based crew with hierarchical process manager	3	[299, 2026]; [306, 2026]; [312, 2026]
module section	AGEINT Design Patterns and Archetypes - Pattern 7: The Debate Agent — Adversarial multi-agent reasoning	1	[147, 2026]
module section	AGEINT Design Patterns and Archetypes - Methods: Devil's Advocacy automation, competing hypotheses generation	2	[297, 2026]; [298, 2026]
module section	AGEINT Design Patterns and Archetypes - Application: Automated Analysis of Competing Hypotheses (ACH)	2	[297, 2026]; [298, 2026]
module section	AGEINT Design Patterns and Archetypes - Code Archetype: AutoGen two-agent debate pattern with judge agent	3	[299, 2026]; [306, 2026]; [312, 2026]
module section	AGEINT Design Patterns and Archetypes - Pattern 8: The RAG-Operator — Retrieval-Augmented Generation over intelligence corpora	1	[148, 2026]
module section	AGEINT Design Patterns and Archetypes - Methods: Dense vector retrieval, hybrid BM25+dense, re-ranking	3	[299, 2026]; [306, 2026]; [312, 2026]
module section	AGEINT Design Patterns and Archetypes - Application: All-source fusion from live document collections	3	[309, 2026]; [310, 2026]; [300, 2026]
module section	AGEINT Design Patterns and Archetypes - Code Archetype: LangChain RAG with Chroma/Pinecone over STIX feeds	3	[309, 2026]; [310, 2026]; [300, 2026]
module section	AGEINT Design Patterns and Archetypes - Pattern 9: The Memory-State Machine — Persistent episodic memory agent	1	[138, 2026]
module section	AGEINT Design Patterns and Archetypes - Methods: Episodic memory write/read, consolidation, attention-weighted retrieval	3	[299, 2026]; [306, 2026]; [312, 2026]
module section	AGEINT Design Patterns and Archetypes - Application: Long-term asset tracking, longitudinal pattern-of-life analysis	3	[299, 2026]; [306, 2026]; [312, 2026]
module section	AGEINT Design Patterns and Archetypes - Code Archetype: LangGraph with PostgreSQL episodic memory and mem0/MemGPT	3	[299, 2026]; [306, 2026]; [312, 2026]
module section	AGEINT Design Patterns and Archetypes - Pattern 10: The Control Plane Agent — Modular tool routing through single interface	1	[145, 2026]
module section	AGEINT Design Patterns and Archetypes - Methods: "Control Plane as a Tool" abstraction, modular routing logic	3	[309, 2026]; [310, 2026]; [300, 2026]
module section	AGEINT Design Patterns and Archetypes - Application: Scalable multi-source collection with single interface	3	[309, 2026]; [310, 2026]; [300, 2026]

Section	Module and source section	Citations	Citation links
module section	AGEINT Design Patterns and Archetypes - Code Archetype: FastAPI meta-tool endpoint wrapping N sub-tools	3	[299, 2026]; [306, 2026]; [312, 2026]
module section	AGEINT Design Patterns and Archetypes - Pattern 11: The Surveillance Agent — Continuous monitoring and alerting	3	[299, 2026]; [306, 2026]; [312, 2026]
module section	AGEINT Design Patterns and Archetypes - Methods: Scheduled polling, anomaly detection, threshold alerting	3	[309, 2026]; [310, 2026]; [300, 2026]
module section	AGEINT Design Patterns and Archetypes - Application: Persistent target monitoring, dark web alerting, infrastructure tracking	3	[299, 2026]; [306, 2026]; [312, 2026]
module section	AGEINT Design Patterns and Archetypes - Code Archetype: n8n or LangGraph cron-triggered agent with Shodan/SpiderFoot APIs	3	[307, 2026]; [305, 2026]; [304, 2026]
module section	AGEINT Design Patterns and Archetypes - Pattern 12: The Red Team Agent — Adversarial attack simulation	1	[147, 2026]
module section	AGEINT Design Patterns and Archetypes - Methods: Adversarial prompt generation, attack-tree traversal, kill chain simulation	3	[300, 2026]; [304, 2026]; [306, 2026]
module section	AGEINT Design Patterns and Archetypes - Application: Penetration testing automation, vulnerability discovery	3	[300, 2026]; [304, 2026]; [306, 2026]
module section	AGEINT Design Patterns and Archetypes - Code Archetype: AutoGen code execution agent with MITRE ATT&CK tool plugin	3	[300, 2026]; [304, 2026]; [306, 2026]
module section	AGEINT Design Patterns and Archetypes - Pattern 13: The Cover Story Generator — Legend and cover document creation	3	[299, 2026]; [306, 2026]; [312, 2026]
module section	AGEINT Design Patterns and Archetypes - Methods: Persona generation, document synthesis, consistency checking	3	[299, 2026]; [306, 2026]; [312, 2026]
module section	AGEINT Design Patterns and Archetypes - Application: NOC legend maintenance, sock puppet operational security	3	[299, 2026]; [306, 2026]; [312, 2026]
module section	AGEINT Design Patterns and Archetypes - Code Archetype: GPT-4o with structured output schemas for persona consistency	3	[299, 2026]; [306, 2026]; [312, 2026]
module section	AGEINT Design Patterns and Archetypes - Pattern 14: The Deception Detector — Verification and source reliability agent	3	[299, 2026]; [306, 2026]; [312, 2026]
module section	AGEINT Design Patterns and Archetypes - Methods: Cross-source triangulation, metadata analysis, deepfake detection API calls	3	[309, 2026]; [310, 2026]; [300, 2026]
module section	AGEINT Design Patterns and Archetypes - Application: Source vetting, product validation, disinformation identification	2	[308, 2026]; [311, 2026]

Section	Module and source section	Citations	Citation links
module section	AGEINT Design Patterns and Archetypes - Code Archetype: LangChain agent with Hive Moderation, Sightengine, C2PA APIs	3	[299, 2026]; [306, 2026]; [312, 2026]
module section	AGEINT Design Patterns and Archetypes - Pattern 15: The Analyst in the Loop — Human-in-the-loop (HITL) intelligence agent	1	[004, 2026]
module section	AGEINT Design Patterns and Archetypes - Methods: Interrupt-and-query, confidence-gated human escalation	2	[297, 2026]; [298, 2026]
module section	AGEINT Design Patterns and Archetypes - Application: Supervised analysis; compliance-constrained environments	3	[299, 2026]; [306, 2026]; [312, 2026]
module section	AGEINT Design Patterns and Archetypes - Code Archetype: LangGraph with human_approval node and async interrupt handlers	3	[299, 2026]; [306, 2026]; [312, 2026]
module section	AGEINT Design Patterns and Archetypes - Pattern 16: The Cyber Sentinel — Autonomous threat intelligence and response	2	[149, 2026]; [150, 2026]
module section	AGEINT Design Patterns and Archetypes - Methods: SIEM integration, SOAR automation, ATT&CK technique mapping	2	[302, 2026]; [297, 2026]
module section	AGEINT Design Patterns and Archetypes - Application: Autonomous SOC tier-1 triage, IOC enrichment	3	[299, 2026]; [306, 2026]; [312, 2026]
module section	AGEINT Design Patterns and Archetypes - Code Archetype: CrewAI crew with Splunk/Elastic SIEM tools and STIX/TAXII writer	3	[309, 2026]; [310, 2026]; [300, 2026]
module section	AGEINT Design Patterns and Archetypes - Pattern 17: The Supply Chain Inspector — Software provenance and integrity agent	3	[303, 2026]; [304, 2026]; [305, 2026]
module section	AGEINT Design Patterns and Archetypes - Methods: SBOM parsing, dependency graph analysis, commit diff analysis	3	[303, 2026]; [304, 2026]; [305, 2026]
module section	AGEINT Design Patterns and Archetypes - Application: Open-source supply chain threat hunting (post-XZ Utils)	1	[076, 2026]
module section	AGEINT Design Patterns and Archetypes - Code Archetype: Python agent with Syft/Grype SBOM tools and GitHub commit analysis	3	[303, 2026]; [304, 2026]; [305, 2026]
module section	AGEINT Design Patterns and Archetypes - Pattern 18: The GEOINT Analyst — Automated satellite imagery analysis	2	[302, 2026]; [297, 2026]
module section	AGEINT Design Patterns and Archetypes - Methods: Vision model object detection, change detection, chronolocation	2	[302, 2026]; [297, 2026]
module section	AGEINT Design Patterns and Archetypes - Application: Facility monitoring, order-of-battle assessment	3	[299, 2026]; [306, 2026]; [312, 2026]

Section	Module and source section	Citations	Citation links
module section	AGEINT Design Patterns and Archetypes - Code Archetype: GPT-4o Vision + Google Earth Engine API + LangChain agent loop	3	[299, 2026]; [306, 2026]; [312, 2026]
module section	AGEINT Design Patterns and Archetypes - Pattern 19: The Cognitive Inoculant — Prebunking and cognitive resilience agent	1	[151, 2026]
module section	AGEINT Design Patterns and Archetypes - Methods: Manipulation technique detection, inoculation content generation, user adaptation	2	[308, 2026]; [311, 2026]
module section	AGEINT Design Patterns and Archetypes - Application: Population-scale cognitive security intervention delivery	1	[152, 2026]
module section	AGEINT Design Patterns and Archetypes - Code Archetype: LangChain agent with CAMBREX taxonomy + API delivery pipeline	3	[305, 2026]; [304, 2026]; [303, 2026]
module section	AGEINT Design Patterns and Archetypes - Pattern 20: The Hierarchical Command — Orchestrator-subagent architecture	2	[139, 2026]; [137, 2026]
module section	AGEINT Design Patterns and Archetypes - Methods: Goal decomposition, subagent delegation, output aggregation, failure recovery	3	[299, 2026]; [306, 2026]; [312, 2026]
module section	AGEINT Design Patterns and Archetypes - Application: Complex multi-domain operations with role separation	3	[299, 2026]; [306, 2026]; [312, 2026]
module section	AGEINT Design Patterns and Archetypes - Code Archetype: LangGraph supervisor pattern with specialized subagent nodes	3	[299, 2026]; [306, 2026]; [312, 2026]
33.99	AGEINT Frameworks and Infrastructure - V2 source-lane extension: bind AGEINT Frameworks and Infrastructure to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[255, 2026]; [256, 2026]; [258, 2026]
33.100	AGEINT Frameworks and Infrastructure - V2 AGEINT-depth extension: map frameworks to interoperable tool descriptions, Web of Things affordances, OpenAPI contracts, credential semantics, revocation, and error-handling evidence	3	[255, 2026]; [256, 2026]; [258, 2026]
33.101	AGEINT Frameworks and Infrastructure - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for AGEINT Frameworks and Infrastructure	3	[273, 2026]; [274, 2026]; [275, 2026]

Section	Module and source section	Citations	Citation links
33.102	AGEINT Frameworks and Infrastructure - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for AGEINT Frameworks and Infrastructure	3	[286, 2026]; [287, 2026]; [292, 2026]
33.1	AGEINT Frameworks and Infrastructure - LangChain/LangGraph: State Machine Orchestration	2	[147, 2026]; [153, 2026]
33.1.1	AGEINT Frameworks and Infrastructure - LCEL: LangChain Expression Language	3	[299, 2026]; [306, 2026]; [312, 2026]
33.1.2	AGEINT Frameworks and Infrastructure - LangGraph: Stateful, Cyclical Agentic Workflows	3	[299, 2026]; [306, 2026]; [312, 2026]
33.1.3	AGEINT Frameworks and Infrastructure - LangSmith: Observability and Tracing	3	[299, 2026]; [306, 2026]; [312, 2026]
33.2	AGEINT Frameworks and Infrastructure - CrewAI: Role-Based Multi-Agent Collaboration	2	[154, 2026]; [153, 2026]
33.2.1	AGEINT Frameworks and Infrastructure - Crew, Agent, Task, and Process Objects	3	[299, 2026]; [306, 2026]; [312, 2026]
33.2.2	AGEINT Frameworks and Infrastructure - Sequential, Parallel, and Hierarchical Process Modes	3	[299, 2026]; [306, 2026]; [312, 2026]
33.2.3	AGEINT Frameworks and Infrastructure - Built-in Tool Ecosystem	3	[299, 2026]; [306, 2026]; [312, 2026]
33.3	AGEINT Frameworks and Infrastructure - AutoGen (Microsoft): Multi-Agent Conversation Patterns	2	[147, 2026]; [153, 2026]
33.3.1	AGEINT Frameworks and Infrastructure - AssistantAgent and UserProxyAgent Pattern	3	[299, 2026]; [306, 2026]; [312, 2026]
33.3.2	AGEINT Frameworks and Infrastructure - GroupChat with RoundRobin and AutoSelect Managers	3	[299, 2026]; [306, 2026]; [312, 2026]
33.3.3	AGEINT Frameworks and Infrastructure - Code Execution Risk and Sandboxing Requirements	1	[147, 2026]
33.4	AGEINT Frameworks and Infrastructure - Semantic Kernel: Enterprise AI Orchestration	1	[147, 2026]
33.5	AGEINT Frameworks and Infrastructure - AWS Agentic Patterns: Production Architecture Guide	1	[144, 2026]
33.5.1	AGEINT Frameworks and Infrastructure - Basic Reasoning Agents	3	[299, 2026]; [306, 2026]; [312, 2026]
33.5.2	AGEINT Frameworks and Infrastructure - Tool-Based Agents (Function Calling and MCP Servers)	3	[299, 2026]; [306, 2026]; [312, 2026]
33.5.3	AGEINT Frameworks and Infrastructure - Computer-Use Agents	3	[299, 2026]; [306, 2026]; [312, 2026]
33.5.4	AGEINT Frameworks and Infrastructure - Coding Agents	3	[299, 2026]; [306, 2026]; [312, 2026]

Section	Module and source section	Citations	Citation links
33.5.5	AGEINT Frameworks and Infrastructure - Speech-to-Speech Agents	3	[299, 2026]; [306, 2026]; [312, 2026]
33.5.6	AGEINT Frameworks and Infrastructure - Orchestration Patterns: Supervisor, Parallel, Subgraph	3	[299, 2026]; [306, 2026]; [312, 2026]
33.6	AGEINT Frameworks and Infrastructure - Model Context Protocol (MCP): The USB Standard for Agentic AI	4	[155, 2026]; [156, 2026]; [157, 2026]; [158, 2026]
33.6.1	AGEINT Frameworks and Infrastructure - MCP Architecture: Client, Server, Host	3	[299, 2026]; [306, 2026]; [312, 2026]
33.6.2	AGEINT Frameworks and Infrastructure - NSA Security Design Considerations for MCP	1	[155, 2026]
33.6.3	AGEINT Frameworks and Infrastructure - MCP Security Risks: Tool Poisoning, Prompt Injection via Server	1	[159, 2026]
33.6.4	AGEINT Frameworks and Infrastructure - MCP in Intelligence Workflows: Structured Tool Registration	3	[299, 2026]; [306, 2026]; [312, 2026]
33.7	AGEINT Frameworks and Infrastructure - Agent-to-Agent (A2A) Protocols: Interoperability Between Frameworks	1	[137, 2026]
33.8	AGEINT Frameworks and Infrastructure - n8n and Make.com: No-Code/Low-Code Agentic Intelligence Pipelines	1	[153, 2026]

80.6 Add or extend a citation: preserve identity and record metadata (continued 2)

Section	Module and source section	Citations	Citation links
33.9	AGEINT Frameworks and Infrastructure - Top 8 Agentic AI Frameworks Comparison (2026)	1	[146, 2026]
34.99	AGEINT Security and Adversarial Considerations - V2 source-lane extension: bind AGEINT Security and Adversarial Considerations to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[234, 2026]; [235, 2026]; [236, 2026]
34.100	AGEINT Security and Adversarial Considerations - V2 AGEINT-depth extension: require compliance mapping, adversarial evaluation, impact assessment, trustworthiness review, and accountable remediation for agent security discussions	3	[234, 2026]; [235, 2026]; [236, 2026]
34.101	AGEINT Security and Adversarial Considerations - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for AGEINT Security and Adversarial Considerations	3	[276, 2026]; [277, 2026]; [284, 2026]
34.102	AGEINT Security and Adversarial Considerations - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for AGEINT Security and Adversarial Considerations	3	[288, 2026]; [289, 2026]; [293, 2026]
34.1	AGEINT Security and Adversarial Considerations - Agent Framework Security Vulnerabilities	1	[147, 2026]
34.1.1	AGEINT Security and Adversarial Considerations - LangChain PythonREPLTool: Arbitrary Code Execution	3	[299, 2026]; [306, 2026]; [312, 2026]
34.1.2	AGEINT Security and Adversarial Considerations - CrewAI Uncontrolled Lateral Movement Between Agents	3	[299, 2026]; [306, 2026]; [312, 2026]
34.1.3	AGEINT Security and Adversarial Considerations - AutoGen Unsandboxed Code Execution	1	[147, 2026]
34.1.4	AGEINT Security and Adversarial Considerations - MCP Server Poisoning and Prompt Injection	2	[155, 2026]; [159, 2026]
34.2	AGEINT Security and Adversarial Considerations - Prompt Injection in Intelligence Agentic Systems	1	[137, 2026]

Section	Module and source section	Citations	Citation links
34.3	AGEINT Security and Adversarial Considerations - Hallucination in Action: When Agents Act on Fabricated Intelligence	1	[137, 2026]
34.4	AGEINT Security and Adversarial Considerations - Infinite Loops and Runaway Agents: Detection and Kill Switches	1	[137, 2026]
34.5	AGEINT Security and Adversarial Considerations - Agentic AI Governance Frameworks 2026	2	[160, 2026]; [161, 2026]
34.5.1	AGEINT Security and Adversarial Considerations - OWASP Top 10 for LLM Applications	3	[299, 2026]; [306, 2026]; [312, 2026]
34.5.2	AGEINT Security and Adversarial Considerations - IAPS Agentic AI Governance Framework	3	[299, 2026]; [306, 2026]; [312, 2026]
34.5.3	AGEINT Security and Adversarial Considerations - UK AI Safety Institute: Agent Evaluations	3	[299, 2026]; [306, 2026]; [312, 2026]
34.6	AGEINT Security and Adversarial Considerations - LLM-Based Agents in Autonomous Cyberattacks: Survey and Taxonomy	1	[100, 2026]
34.6.1	AGEINT Security and Adversarial Considerations - Threat Intelligence Gathering by LLM Agents	1	[100, 2026]
34.6.2	AGEINT Security and Adversarial Considerations - Automated Weaponization: Malware Generation	1	[100, 2026]
34.6.3	AGEINT Security and Adversarial Considerations - Phishing and Spear-Phishing Automation	1	[100, 2026]
34.6.4	AGEINT Security and Adversarial Considerations - Multi-Agent Collaboration in Cyberattacks	1	[100, 2026]
34.6.5	AGEINT Security and Adversarial Considerations - Cyberattack Capabilities Across 6G, IoT, Satellite, UAV Networks	1	[100, 2026]
34.7	AGEINT Security and Adversarial Considerations - Observability as Control: Tracing, Logging, Audit for AGEINT Systems	1	[162, 2026]
34.8	AGEINT Security and Adversarial Considerations - Human-in-the-Loop Architectures: When and How to Mandate Oversight	2	[162, 2026]; [004, 2026]
34.9	AGEINT Security and Adversarial Considerations - Alignment and Trustworthiness in AGEINT: National Security Context	1	[148, 2026]
35.99	Active Inference and AGEINT - V2 source-lane extension: bind Active Inference and AGEINT to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[247, 2026]; [248, 2026]; [265, 2026]

Section	Module and source section	Citations	Citation links
35.100	Active Inference and AGEINT - V2 AGEINT-depth extension: connect active-inference planning to public-sector service adoption, workforce impact, skills governance, and human-centered oversight rather than autonomous agency	3	[247, 2026]; [248, 2026]; [265, 2026]
35.101	Active Inference and AGEINT - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Active Inference and AGEINT	3	[278, 2026]; [279, 2026]; [283, 2026]
35.102	Active Inference and AGEINT - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Active Inference and AGEINT	3	[290, 2026]; [291, 2026]; [294, 2026]
35.1	Active Inference and AGEINT - The Free Energy Principle and Predictive Processing	1	[106, 2026]
35.2	Active Inference and AGEINT - Active Inference as Computational Model of Intelligence Agent Behavior	1	[003, 2026]
35.3	Active Inference and AGEINT - Shared Protentions in Multi-Agent Active Inference	1	[163, 2026]
35.4	Active Inference and AGEINT - Active Inference for Social Organization and Intelligence Communities	1	[003, 2026]
35.5	Active Inference and AGEINT - VERSES AI Research: Multi-Scale Active Inference Architectures	2	[163, 2026]; [164, 2026]
35.6	Active Inference and AGEINT - Cognitive Security Through the Active Inference Lens	1	[105, 2026]
35.7	Active Inference and AGEINT - Applications: Deception Detection, Surprise Minimization, Threat Modeling	3	[309, 2026]; [310, 2026]; [300, 2026]
35.8	Active Inference and AGEINT - Applications of Active Inference and FEP in Intelligence (TU Delft Thesis)	1	[106, 2026]
36.99	AGEINT Python Code Library - V2 source-lane extension: bind AGEINT Python Code Library to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[242, 2026]; [243, 2026]; [246, 2026]

Section	Module and source section	Citations	Citation links
36.100	AGEINT Python Code Library - V2 AGEINT-depth extension: convert code-library material into education-safe capstone workflows with instructor rubrics, prompt transparency, allowed tools, and human override requirements	3	[242, 2026]; [243, 2026]; [246, 2026]
36.101	AGEINT Python Code Library - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for AGEINT Python Code Library	3	[280, 2026]; [281, 2026]; [282, 2026]
36.102	AGEINT Python Code Library - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for AGEINT Python Code Library	3	[292, 2026]; [295, 2026]; [296, 2026]
36.1	AGEINT Python Code Library - Threat Intelligence Aggregation Agent: LangChain + STIX/TAXII	3	[309, 2026]; [310, 2026]; [300, 2026]
36.2	AGEINT Python Code Library - Multi-Agent OSINT Crew: CrewAI + Shodan + theHarvester + Maltego	2	[301, 2026]; [298, 2026]
36.3	AGEINT Python Code Library - Autonomous Vulnerability Scanner: AutoGen + Nmap + MITRE ATT&CK Navigator	3	[300, 2026]; [304, 2026]; [306, 2026]
36.4	AGEINT Python Code Library - RAG Pipeline for All-Source Intelligence Fusion: LangGraph + Chroma + OpenAI	3	[305, 2026]; [304, 2026]; [303, 2026]
36.5	AGEINT Python Code Library - Pattern-of-Life Analysis Agent: Persistent Memory + GEOINT + OSINT	2	[301, 2026]; [298, 2026]
36.6	AGEINT Python Code Library - Cognitive Security Inoculation Agent: Van der Linden Taxonomy + GPT-4o	2	[308, 2026]; [311, 2026]
36.7	AGEINT Python Code Library - Supply Chain Inspector: SBOM + GitHub Commit Analysis + Anomaly Detection	3	[303, 2026]; [304, 2026]; [305, 2026]
36.8	AGEINT Python Code Library - ICS Anomaly Detection Agent: OT Network + MITRE ATT&CK for ICS	3	[307, 2026]; [305, 2026]; [304, 2026]

Section	Module and source section	Citations	Citation links
37.99	Cognitive Security: Foundations and Definitions - V2 source-lane extension: bind Cognitive Security: Foundations and Definitions to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[238, 2026]; [239, 2026]; [244, 2026]
37.101	Cognitive Security: Foundations and Definitions - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Cognitive Security: Foundations and Definitions	3	[273, 2026]; [276, 2026]; [285, 2026]
37.102	Cognitive Security: Foundations and Definitions - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Cognitive Security: Foundations and Definitions	3	[286, 2026]; [290, 2026]; [294, 2026]
37.1	Cognitive Security: Foundations and Definitions - What Is Cognitive Security? Definitions, Scope, Emergence	3	[165, 2026]; [166, 2026]; [167, 2026]
37.1.1	Cognitive Security: Foundations and Definitions - Comprehensive Definition: State and Process Against Malign Influence	1	[166, 2026]
37.1.2	Cognitive Security: Foundations and Definitions - Cognitive Security vs. Cybersecurity vs. Information Security	1	[095, 2026]
37.1.3	Cognitive Security: Foundations and Definitions - Three Pillars: Awareness + Situation Awareness + Purposeful Action	1	[166, 2026]
37.2	Cognitive Security: Foundations and Definitions - Unveiling the Multifaceted Concept of Cognitive Security (Elsevier, 2025)	2	[165, 2026]; [167, 2026]
37.3	Cognitive Security: Foundations and Definitions - Cognitive Security in the Age of AI (RESAID Policy Paper, 2025)	1	[095, 2026]
37.4	Cognitive Security: Foundations and Definitions - AI Development Should Prioritize Cognitive Security (NeurIPS Position Paper, 2023)	1	[096, 2026]
37.4.1	Cognitive Security: Foundations and Definitions - DARPA Intrinsic Cognitive Security (ICS) Program	3	[168, 2026]; [169, 2026]; [170, 2026]

Section	Module and source section	Citations	Citation links
37.4.2	Cognitive Security: Foundations and Definitions - Mixed Reality Cognitive Attack Typology	1	[171, 2026]
37.4.3	Cognitive Security: Foundations and Definitions - Formal Methods for Cognitive Guarantees in MR Systems	1	[169, 2026]
37.5	Cognitive Security: Foundations and Definitions - Behavioral Outcomes of Human Cognitive Security (arXiv, March 2026)	1	[107, 2026]
37.6	Cognitive Security: Foundations and Definitions - Defining Comprehensive Cognitive Security in the Digital Era (SSRN 2024)	1	[166, 2026]
37.7	Cognitive Security: Foundations and Definitions - Ethics of Cognitive Security (YorkSpace Dissertation)	1	[172, 2026]
37.8	Cognitive Security: Foundations and Definitions - Epistemic Security: Protecting Knowledge Production and Distribution	3	[307, 2026]; [305, 2026]; [304, 2026]
37.8.1	Cognitive Security: Foundations and Definitions - Seger: Epistemic Security as a Field	1	[173, 2026]
37.8.2	Cognitive Security: Foundations and Definitions - Epistemic Security 2029: Fortifying the UK's Information Supply Chain	1	[174, 2026]
37.8.3	Cognitive Security: Foundations and Definitions - Tackling Threats to Informed Decision-Making (Turing Institute)	1	[175, 2026]
37.8.4	Cognitive Security: Foundations and Definitions - Epistemic Governance in Crisis: A Complexity Approach	1	[001, 2026]
38.99	Neurocognitive Mechanisms of Cognitive Security - V2 source-lane extension: bind Neurocognitive Mechanisms of Cognitive Security to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[238, 2026]; [240, 2026]; [244, 2026]
38.101	Neurocognitive Mechanisms of Cognitive Security - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Neurocognitive Mechanisms of Cognitive Security	3	[274, 2026]; [278, 2026]; [280, 2026]

Section	Module and source section	Citations	Citation links
38.102	Neurocognitive Mechanisms of Cognitive Security - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Neurocognitive Mechanisms of Cognitive Security	3	[287, 2026]; [288, 2026]; [295, 2026]
38.1	Neurocognitive Mechanisms of Cognitive Security - Understanding Neurocognitive Mechanisms of Cognitive Security (Neuroscience & Biobehavioral Reviews, 2025)	2	[176, 2026]; [177, 2026]
38.1.1	Neurocognitive Mechanisms of Cognitive Security - Executive Brain Systems and Vulnerability to Information Threats	1	[177, 2026]
38.1.2	Neurocognitive Mechanisms of Cognitive Security - Affective Systems: Emotional Exploitation in Manipulation	1	[177, 2026]
38.1.3	Neurocognitive Mechanisms of Cognitive Security - Integrative Systems: Brain Network Interactions During Threat Exposure	1	[177, 2026]
38.1.4	Neurocognitive Mechanisms of Cognitive Security - Neuromarkers of Susceptibility and Resilience	1	[177, 2026]
38.2	Neurocognitive Mechanisms of Cognitive Security - Neuro-Cognitive Approaches to Cybersecurity: Systematic Review (Emerald, 2025)	1	[178, 2026]
38.3	Neurocognitive Mechanisms of Cognitive Security - Cognitive Load in Intelligence Community Settings (NCSU Survey, 2024)	1	[179, 2026]
38.3.1	Neurocognitive Mechanisms of Cognitive Security - 129 Metrics Catalogued: Questionnaire, Biometric, Task-Performance	1	[179, 2026]
38.3.2	Neurocognitive Mechanisms of Cognitive Security - NASA-TLX and Its Intelligence Analytic Applications	1	[179, 2026]
38.3.3	Neurocognitive Mechanisms of Cognitive Security - Eye Tracking and Heart Rate Variability for Analyst Overload Detection	1	[179, 2026]
38.4	Neurocognitive Mechanisms of Cognitive Security - Information Overload and Cognitive Bias in Intelligence Analysis	1	[180, 2026]
38.5	Neurocognitive Mechanisms of Cognitive Security - Decision-Making Under Uncertainty: Neural Mechanisms and Intelligence Implications	2	[308, 2026]; [311, 2026]

Section	Module and source section	Citations	Citation links
39.99	Psychological Inoculation and Prebunking - V2 source-lane extension: bind Psychological Inoculation and Prebunking to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[242, 2026]; [243, 2026]; [245, 2026]
39.101	Psychological Inoculation and Prebunking - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Psychological Inoculation and Prebunking	3	[279, 2026]; [282, 2026]; [284, 2026]
39.102	Psychological Inoculation and Prebunking - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Psychological Inoculation and Prebunking	3	[289, 2026]; [291, 2026]; [296, 2026]
39.1	Psychological Inoculation and Prebunking - Inoculation Theory: McGuire and Papageorgis (1961) to Present	2	[181, 2026]; [182, 2026]
39.2	Psychological Inoculation and Prebunking - Psychological Inoculation Against Misinformation: Meta-Analysis	1	[182, 2026]
39.3	Psychological Inoculation and Prebunking - Prebunking Interventions Based on Inoculation Theory (Harvard Kennedy School)	1	[183, 2026]
39.4	Psychological Inoculation and Prebunking - Cambridge/Jigsaw YouTube Field Study: 5.4 Million Users, 7 Experiments	1	[152, 2026]
39.4.1	Psychological Inoculation and Prebunking - Inoculation Effect: Measured Improvement in Manipulation Recognition	1	[152, 2026]
39.4.2	Psychological Inoculation and Prebunking - Source-Agnostic Design: Effective Across Political Affiliations	1	[152, 2026]
39.4.3	Psychological Inoculation and Prebunking - Scaling at $0.05 Per View; Campaign Applications	1	[152, 2026]
39.5	Psychological Inoculation and Prebunking - Psychological Inoculation (JNNP, van der Linden 2023)	1	[184, 2026]
39.6	Psychological Inoculation and Prebunking - “Inoculation” to Resist Misinformation (JAMA, 2024)	1	[185, 2026]

Section	Module and source section	Citations	Citation links
39.7	Psychological Inoculation and Prebunking - Psychological Inoculation Against Misinformation: Current Evidence and Boundary Conditions (ANNALS, 2022)	1	[186, 2026]
39.8	Psychological Inoculation and Prebunking - NATO STRATCOM COE: Inoculation Theory and Misinformation (PDF)	1	[187, 2026]
39.9	Psychological Inoculation and Prebunking - A Practical Guide to Prebunking (Cambridge/Jigsaw/BBC)	1	[151, 2026]
39.10	Psychological Inoculation and Prebunking - Critical Thinking Training vs. Misinformation: Systematic Review (Nature Comms, 2025)	1	[181, 2026]
39.11	Psychological Inoculation and Prebunking - Operationalizing Prebunking in AGEINT: Transparent Resilience Education and	2	[308, 2026]; [311, 2026]
40.99	Cognitive Security Operations - V2 source-lane extension: bind Cognitive Security Operations to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[238, 2026]; [239, 2026]; [246, 2026]
40.101	Cognitive Security Operations - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Cognitive Security Operations	3	[275, 2026]; [276, 2026]; [283, 2026]
40.102	Cognitive Security Operations - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Cognitive Security Operations	3	[286, 2026]; [293, 2026]; [295, 2026]
40.1	Cognitive Security Operations - The Cognitive Attack Surface: Attention, Memory, Trust, and Decision-Making	1	[095, 2026]
40.2	Cognitive Security Operations - Adversarial Cognitive Operations: PSYOP, Active Measures, Synthetic Influence	1	[105, 2026]
40.3	Cognitive Security Operations - Deepfakes, Voice Cloning, and Digital Identity Attacks	3	[300, 2026]; [304, 2026]; [306, 2026]
40.4	Cognitive Security Operations - From Spycraft to Self-Mastery: SATs for Personal Cognitive Security	1	[188, 2026]

Section	Module and source section	Citations	Citation links
40.5	Cognitive Security Operations - Building Organizational Cognitive Resilience	1	[095, 2026]
40.6	Cognitive Security Operations - National Cognitive Security Centers: Policy Proposals	1	[095, 2026]
40.7	Cognitive Security Operations - Cognitive Security and Active Inference: The Predictive Mind Under Attack	2	[106, 2026]; [003, 2026]
40.8	Cognitive Security Operations - AI-Assisted Cognitive Security Tools: Detection and Intervention Systems	1	[096, 2026]
41.99	Structured Analytic Techniques (SATs) - V2 source-lane extension: bind Structured Analytic Techniques (SATs) to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[237, 2026]; [266, 2026]; [269, 2026]
41.101	Structured Analytic Techniques (SATs) - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Structured Analytic Techniques (SATs)	3	[273, 2026]; [274, 2026]; [275, 2026]
41.102	Structured Analytic Techniques (SATs) - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Structured Analytic Techniques (SATs)	3	[286, 2026]; [287, 2026]; [292, 2026]
41.1	Structured Analytic Techniques (SATs) - CIA Tradecraft Primer: SATs for Intelligence Analysis	2	[189, 2026]; [108, 2026]
41.2	Structured Analytic Techniques (SATs) - ICD 203 Analytic Standards: The Nine Tradecraft Standards	2	[002, 2026]; [190, 2026]
41.3	Structured Analytic Techniques (SATs) - Psychology of Intelligence Analysis (Heuer, CIA 1999)	3	[180, 2026]; [191, 2026]; [192, 2026]
41.4	Structured Analytic Techniques (SATs) - Structured Analytic Techniques (Heuer & Pherson, 2011)	2	[193, 2026]; [194, 2026]
41.4.1	Structured Analytic Techniques (SATs) - Analysis of Competing Hypotheses (ACH)	2	[297, 2026]; [298, 2026]
41.4.2	Structured Analytic Techniques (SATs) - Devil's Advocacy and Red Teaming	3	[300, 2026]; [304, 2026]; [306, 2026]

Section	Module and source section	Citations	Citation links
41.4.3	Structured Analytic Techniques (SATs) - Alternative Futures Analysis	2	[297, 2026]; [298, 2026]
41.4.4	Structured Analytic Techniques (SATs) - Brainstorming and Divergent Thinking Techniques	2	[297, 2026]; [298, 2026]
41.4.5	Structured Analytic Techniques (SATs) - Deception Detection SATs	1	[193, 2026]
41.4.6	Structured Analytic Techniques (SATs) - Key Assumptions Check	2	[297, 2026]; [298, 2026]
41.4.7	Structured Analytic Techniques (SATs) - Indicators Validator	3	[309, 2026]; [310, 2026]; [300, 2026]
41.4.8	Structured Analytic Techniques (SATs) - What If? / Pre-Mortem Analysis	2	[297, 2026]; [298, 2026]
41.5	Structured Analytic Techniques (SATs) - Analytic Tradecraft and the Intelligence Community (Tandfonline, 2014)	1	[195, 2026]
41.6	Structured Analytic Techniques (SATs) - Analytic Tradecraft Standards in Army Intelligence	1	[196, 2026]
41.7	Structured Analytic Techniques (SATs) - Cognitive Biases: Confirmation Bias, Anchoring, Groupthink in Intelligence	1	[180, 2026]
41.8	Structured Analytic Techniques (SATs) - From Spycraft to Self-Mastery: SATs for Everyday Decision-Making	1	[188, 2026]
42.99	Advanced Analysis Methods - V2 source-lane extension: bind Advanced Analysis Methods to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[237, 2026]; [266, 2026]; [270, 2026]
42.101	Advanced Analysis Methods - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Advanced Analysis Methods	3	[276, 2026]; [277, 2026]; [284, 2026]
42.102	Advanced Analysis Methods - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Advanced Analysis Methods	3	[288, 2026]; [289, 2026]; [293, 2026]
42.1	Advanced Analysis Methods - Red Cell Analysis and Adversarial Wargaming	3	[300, 2026]; [304, 2026]; [306, 2026]
42.2	Advanced Analysis Methods - Network Analysis: Link Charts, Activity Matrices, Social Network Analysis	3	[309, 2026]; [310, 2026]; [300, 2026]

Section	Module and source section	Citations	Citation links
42.3	Advanced Analysis Methods - Timeline Analysis and Event Sequencing	2	[297, 2026]; [298, 2026]
42.4	Advanced Analysis Methods - Collection Management: Requirements, Gaps, Tasking	3	[309, 2026]; [310, 2026]; [300, 2026]
42.5	Advanced Analysis Methods - Writing Intelligence Products: Assessments, Estimates, Warnings	2	[297, 2026]; [298, 2026]
42.6	Advanced Analysis Methods - Communicating Uncertainty: Analytic Line vs. Raw Reporting	2	[297, 2026]; [298, 2026]
42.7	Advanced Analysis Methods - Machine-Assisted Analysis: When to Automate, When to Require Human Judgment	2	[297, 2026]; [298, 2026]
43.99	The Intelligent Operator as Cognitive Athlete - V2 source-lane extension: bind The Intelligent Operator as Cognitive Athlete to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[262, 2026]; [263, 2026]; [264, 2026]
43.101	The Intelligent Operator as Cognitive Athlete - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for The Intelligent Operator as Cognitive Athlete	3	[278, 2026]; [279, 2026]; [283, 2026]
43.102	The Intelligent Operator as Cognitive Athlete - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for The Intelligent Operator as Cognitive Athlete	3	[290, 2026]; [291, 2026]; [294, 2026]
43.1	The Intelligent Operator as Cognitive Athlete - Productivity Tradecraft: Managing Cognitive Resources for Sustained Operations	2	[308, 2026]; [311, 2026]
43.2	The Intelligent Operator as Cognitive Athlete - The Science Behind Getting Things Done (GTD): Cognitive Foundations	1	[197, 2026]
43.2.1	The Intelligent Operator as Cognitive Athlete - GTD as External Memory and Affordance System	1	[197, 2026]
43.2.2	The Intelligent Operator as Cognitive Athlete - The Five GTD Phases: Capture, Clarify, Organize, Reflect, Engage	1	[198, 2026]

Section	Module and source section	Citations	Citation links
43.2.3	The Intelligent Operator as Cognitive Athlete - Why GTD Improves Team Intelligence Performance (Allen, 2024)	1	[199, 2026]
43.2.4	The Intelligent Operator as Cognitive Athlete - GTD and Reduction of Cognitive Load: Empirical Evidence	2	[179, 2026]; [197, 2026]
43.3	The Intelligent Operator as Cognitive Athlete - Flow State and Peak Performance in Intelligence Work	3	[200, 2026]; [201, 2026]; [202, 2026]
43.3.1	The Intelligent Operator as Cognitive Athlete - Csikszentmihalyi's Flow: Definition, Seven Conditions, Neurophysiology	1	[203, 2026]
43.3.2	The Intelligent Operator as Cognitive Athlete - Neuroscience of Flow: Prefrontal Cortex Deactivation, Dopamine	1	[204, 2026]
43.3.3	The Intelligent Operator as Cognitive Athlete - Flow Research Collective	1	[205, 2026]
43.3.4	The Intelligent Operator as Cognitive Athlete - Go With the Flow: Neuroscientific View on Full Engagement (PMC, 2020)	1	[201, 2026]
43.3.5	The Intelligent Operator as Cognitive Athlete - Investigating the Flow Experience: Key Conceptual Issues (PMC, 2020)	1	[206, 2026]
43.3.6	The Intelligent Operator as Cognitive Athlete - Engineering Flow State for Intelligence Analysis Environments	1	[205, 2026]
43.4	The Intelligent Operator as Cognitive Athlete - Cognitive Load Management in Intelligence Work	1	[179, 2026]
43.4.1	The Intelligent Operator as Cognitive Athlete - Cognitive Load–Productivity Tradeoff in Task Switching	1	[207, 2026]
43.4.2	The Intelligent Operator as Cognitive Athlete - NASA-TLX and Analyst Workload Monitoring	1	[179, 2026]
43.4.3	The Intelligent Operator as Cognitive Athlete - Biometric Monitoring for Real-Time Load Detection	1	[179, 2026]
43.5	The Intelligent Operator as Cognitive Athlete - Spycraft and Cognitive Performance: Inside the Operative's Mind	1	[025, 2026]
43.5.1	The Intelligent Operator as Cognitive Athlete - MICE Framework and Moral Flexibility: Operative Psychology	1	[025, 2026]
43.5.2	The Intelligent Operator as Cognitive Athlete - Trust, Loneliness, and the Psychological Cost of Tradecraft	1	[025, 2026]
43.5.3	The Intelligent Operator as Cognitive Athlete - Pattern Recognition, Not Task Management: Operative Cognitive Design	1	[025, 2026]
43.6	The Intelligent Operator as Cognitive Athlete - Circadian Intelligence: Timing Operations to Peak Cognitive Windows	2	[308, 2026]; [311, 2026]

Section	Module and source section	Citations	Citation links
43.7	The Intelligent Operator as Cognitive Athlete - Adversarial Stress Inoculation: Preparing the Analyst for High-Stakes Environments	3	[300, 2026]; [304, 2026]; [306, 2026]
43.8	The Intelligent Operator as Cognitive Athlete - The Red Zone: How Trauma, PTSD, and Moral Injury Affect Operator Cognition	1	[205, 2026]
44.99	Information Architecture for Intelligence Work - V2 source-lane extension: bind Information Architecture for Intelligence Work to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[251, 2026]; [268, 2026]; [269, 2026]
44.101	Information Architecture for Intelligence Work - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Information Architecture for Intelligence Work	3	[280, 2026]; [281, 2026]; [282, 2026]
44.102	Information Architecture for Intelligence Work - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Information Architecture for Intelligence Work	3	[292, 2026]; [295, 2026]; [296, 2026]
44.1	Information Architecture for Intelligence Work - Personal Knowledge Management (PKM) Systems for Intelligence Professionals	2	[308, 2026]; [311, 2026]
44.1.1	Information Architecture for Intelligence Work - Zettelkasten: German Note-Taking System for Researchers	3	[307, 2026]; [305, 2026]; [304, 2026]
44.1.2	Information Architecture for Intelligence Work - Obsidian, Roam Research, LogSeq: PKM Tools for Analysts	3	[052, 2026]; [051, 2026]; [269, 2026]
44.1.3	Information Architecture for Intelligence Work - Second Brain Methodology Applied to Intelligence Collection	2	[308, 2026]; [311, 2026]
44.2	Information Architecture for Intelligence Work - Information Diet and Source Hygiene	2	[308, 2026]; [311, 2026]
44.3	Information Architecture for Intelligence Work - Distraction Architecture: Designing Environments for Deep Analytical Work	3	[309, 2026]; [310, 2026]; [300, 2026]

Section	Module and source section	Citations	Citation links
44.4	Information Architecture for Intelligence Work - Collaborative Intelligence: Team Workflows, Shared Notes, Secure Platforms	3	[307, 2026]; [305, 2026]; [304, 2026]
44.5	Information Architecture for Intelligence Work - The Analyst's Toolkit: Hardware, Software, and Network Configuration	3	[055, 2026]; [051, 2026]; [301, 2026]
45.99	Industrial Control Systems (ICS) and Operational Technology - V2 source-lane extension: bind Industrial Control Systems (ICS) and Operational Technology to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[255, 2026]; [256, 2026]; [270, 2026]
45.101	Industrial Control Systems (ICS) and Operational Technology - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Industrial Control Systems (ICS) and Operational Technology	3	[273, 2026]; [276, 2026]; [285, 2026]
45.102	Industrial Control Systems (ICS) and Operational Technology - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Industrial Control Systems (ICS) and Operational Technology	3	[286, 2026]; [290, 2026]; [294, 2026]
45.1	Industrial Control Systems (ICS) and Operational Technology - ICS Architecture: SCADA, DCS, PLC, HMI — Definitions and Roles	2	[208, 2026]; [209, 2026]
45.1.1	Industrial Control Systems (ICS) and Operational Technology - SCADA: Supervisory Control and Data Acquisition — Large Geographic Systems	1	[209, 2026]
45.1.2	Industrial Control Systems (ICS) and Operational Technology - DCS: Distributed Control Systems — Chemical, Refining, Power	1	[209, 2026]
45.1.3	Industrial Control Systems (ICS) and Operational Technology - PLC: Programmable Logic Controllers — Field-Level Execution	1	[209, 2026]
45.1.4	Industrial Control Systems (ICS) and Operational Technology - OT vs. IT: Fundamental Security Philosophy Differences	2	[209, 2026]; [210, 2026]

Section	Module and source section	Citations	Citation links
45.1.5	Industrial Control Systems (ICS) and Operational Technology - Air-Gap Erosion: The Digital Transformation Vulnerability	1	[209, 2026]
45.2	Industrial Control Systems (ICS) and Operational Technology - Securing ICS: Components, Protocols, Performance, Vulnerability	1	[208, 2026]
45.3	Industrial Control Systems (ICS) and Operational Technology - 2026 Cybersecurity Guide to ICS (Claroty)	1	[211, 2026]
45.4	Industrial Control Systems (ICS) and Operational Technology - OT vs. ICS vs. SCADA Security (Palo Alto Networks)	1	[210, 2026]
45.5	Industrial Control Systems (ICS) and Operational Technology - Operational Technology Cybersecurity (Idaho National Laboratory)	1	[212, 2026]
46.99	MITRE ATT&CK for ICS - V2 source-lane extension: bind MITRE ATT&CK for ICS to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[255, 2026]; [257, 2026]; [261, 2026]
46.101	MITRE ATT&CK for ICS - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for MITRE ATT&CK for ICS	3	[274, 2026]; [278, 2026]; [280, 2026]
46.102	MITRE ATT&CK for ICS - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for MITRE ATT&CK for ICS	3	[287, 2026]; [288, 2026]; [295, 2026]
46.1	MITRE ATT&CK for ICS - ICS Matrix: 12 Tactics, Full Technique Library	1	[213, 2026]
46.1.1	MITRE ATT&CK for ICS - Initial Access (12 techniques): Drive-by, Remote Services, Wireless Compromise	1	[213, 2026]
46.1.2	MITRE ATT&CK for ICS - Execution: Modify Controller Tasking, Command-Line Interface	1	[213, 2026]
46.1.3	MITRE ATT&CK for ICS - Persistence: Modify Firmware (System and Module), Project File Infection	1	[213, 2026]
46.1.4	MITRE ATT&CK for ICS - Evasion: Rootkit, Masquerading, Indicator Removal	1	[213, 2026]
46.1.5	MITRE ATT&CK for ICS - Discovery: Remote System Discovery, Network Sniffing	1	[213, 2026]

Section	Module and source section	Citations	Citation links
46.1.6	MITRE ATT&CK for ICS - Lateral Movement: Lateral Tool Transfer, Valid Accounts	1	[213, 2026]
46.1.7	MITRE ATT&CK for ICS - Collection: I/O Image, Monitor Process State, Point & Tag Identification	1	[213, 2026]
46.1.8	MITRE ATT&CK for ICS - Inhibit Response Function: Alarm Suppression, Block Communications	1	[213, 2026]
46.1.9	MITRE ATT&CK for ICS - Impair Process Control: Brute Force I/O, Modify Parameter	1	[213, 2026]
46.1.10	MITRE ATT&CK for ICS - Impact: Damage to Property, Loss of Safety, Manipulation of Control	1	[213, 2026]
46.2	MITRE ATT&CK for ICS - Using ICS ATT&CK in Risk Assessment (ISA InTech)	1	[214, 2026]
46.3	MITRE ATT&CK for ICS - Dragos: MITRE ATT&CK for ICS Threat Actor Mapping	1	[215, 2026]
46.4	MITRE ATT&CK for ICS - Nozomi Networks: How Security Teams Use the ICS Framework	1	[216, 2026]
47.99	Historical ICS Cyber Incidents: Intelligence Analysis - V2 source-lane extension: bind Historical ICS Cyber Incidents: Intelligence Analysis to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[252, 2026]; [255, 2026]; [270, 2026]
47.101	Historical ICS Cyber Incidents: Intelligence Analysis - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Historical ICS Cyber Incidents: Intelligence Analysis	3	[279, 2026]; [282, 2026]; [284, 2026]
47.102	Historical ICS Cyber Incidents: Intelligence Analysis - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Historical ICS Cyber Incidents: Intelligence Analysis	3	[289, 2026]; [291, 2026]; [296, 2026]
47.1	Historical ICS Cyber Incidents: Intelligence Analysis - Evaluation Framework for ICS Cyber Incidents (ScienceDirect 2021)	1	[217, 2026]

Section	Module and source section	Citations	Citation links
47.2	Historical ICS Cyber Incidents: Intelligence Analysis - The Cyber-Physical Six: Stuxnet, BlackEnergy, CrashOverride, Trisis, Irongate, Havex	1	[218, 2026]
47.2.1	Historical ICS Cyber Incidents: Intelligence Analysis - Stuxnet: First Cyber-Physical Weapon — Operation Olympic Games	2	[219, 2026]; [220, 2026]
47.2.2	Historical ICS Cyber Incidents: Intelligence Analysis - BlackEnergy: Ukraine Power Grid Attacks (2015)	1	[218, 2026]
47.2.3	Historical ICS Cyber Incidents: Intelligence Analysis - CrashOverride/Industroyer: Protocol-Agnostic Power Grid Weapon	1	[217, 2026]
47.2.4	Historical ICS Cyber Incidents: Intelligence Analysis - Triton/Trisis: Safety Instrumented System Attack	1	[217, 2026]
47.2.5	Historical ICS Cyber Incidents: Intelligence Analysis - Irongate: Stuxnet Descendant Against Simulated Environment	1	[217, 2026]
47.2.6	Historical ICS Cyber Incidents: Intelligence Analysis - Havex: IT-OT Pivot Using Weaponized OPC Software	1	[217, 2026]
47.3	Historical ICS Cyber Incidents: Intelligence Analysis - Threat Scoring Framework: Malware Sophistication × Attack Consequence	1	[217, 2026]
48.99	Threat Intelligence Sharing for Critical Infrastructure - V2 source-lane extension: bind Threat Intelligence Sharing for Critical Infrastructure to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[253, 2026]; [258, 2026]; [261, 2026]
48.101	Threat Intelligence Sharing for Critical Infrastructure - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Threat Intelligence Sharing for Critical Infrastructure	3	[275, 2026]; [276, 2026]; [283, 2026]

Section	Module and source section	Citations	Citation links
48.102	Threat Intelligence Sharing for Critical Infrastructure - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Threat Intelligence Sharing for Critical Infrastructure	3	[286, 2026]; [293, 2026]; [295, 2026]
48.1	Threat Intelligence Sharing for Critical Infrastructure - Evidence-Driven Analysis of Threat Information Sharing for ICS (arXiv 2025)	1	[077, 2026]
48.2	Threat Intelligence Sharing for Critical Infrastructure - ISACs: E-ISAC, WaterISAC, FS-ISAC	3	[307, 2026]; [305, 2026]; [304, 2026]
48.3	Threat Intelligence Sharing for Critical Infrastructure - CISA Frameworks for Critical Infrastructure	3	[307, 2026]; [305, 2026]; [304, 2026]
48.4	Threat Intelligence Sharing for Critical Infrastructure - NERC CIP Standards	3	[307, 2026]; [305, 2026]; [304, 2026]
48.5	Threat Intelligence Sharing for Critical Infrastructure - IDS/IPS for OT Networks: Dragos, Claroty, Nozomi, Armis	3	[307, 2026]; [305, 2026]; [304, 2026]
48.6	Threat Intelligence Sharing for Critical Infrastructure - Honeywell ICS Security: Defense in Depth	1	[218, 2026]
49.99	AGEINT Applied to ICS and Cyber-Physical Intelligence - V2 source-lane extension: bind AGEINT Applied to ICS and Cyber-Physical Intelligence to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[255, 2026]; [256, 2026]; [257, 2026]
49.101	AGEINT Applied to ICS and Cyber-Physical Intelligence - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for AGEINT Applied to ICS and Cyber-Physical Intelligence	3	[273, 2026]; [274, 2026]; [275, 2026]
49.102	AGEINT Applied to ICS and Cyber-Physical Intelligence - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for AGEINT Applied to ICS and Cyber-Physical Intelligence	3	[286, 2026]; [287, 2026]; [292, 2026]

Section	Module and source section	Citations	Citation links
49.1	AGEINT Applied to ICS and Cyber-Physical Intelligence - AI-Driven Anomaly Detection in OT Networks	3	[307, 2026]; [305, 2026]; [304, 2026]
49.2	AGEINT Applied to ICS and Cyber-Physical Intelligence - LLM Agents for ICS Log Analysis and Threat Correlation	3	[299, 2026]; [306, 2026]; [312, 2026]
49.3	AGEINT Applied to ICS and Cyber-Physical Intelligence - Autonomous ICS Incident Response: AGEINT Pattern 16 in OT	1	[213, 2026]
49.4	AGEINT Applied to ICS and Cyber-Physical Intelligence - AGEINT for SCADA Data Fusion and Pattern-of-Process Analysis	3	[307, 2026]; [305, 2026]; [304, 2026]
49.5	AGEINT Applied to ICS and Cyber-Physical Intelligence - Digital Twins for Industrial Intelligence: Simulation and Red Team	3	[300, 2026]; [304, 2026]; [306, 2026]
49.6	AGEINT Applied to ICS and Cyber-Physical Intelligence - Multi-Agent Systems for Critical Infrastructure Protection	3	[299, 2026]; [306, 2026]; [312, 2026]
50.99	Legal Authorities and Constraints - V2 source-lane extension: bind Legal Authorities and Constraints to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[234, 2026]; [238, 2026]; [241, 2026]
50.101	Legal Authorities and Constraints - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Legal Authorities and Constraints	3	[276, 2026]; [277, 2026]; [284, 2026]
50.102	Legal Authorities and Constraints - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Legal Authorities and Constraints	3	[288, 2026]; [289, 2026]; [293, 2026]
50.1	Legal Authorities and Constraints - Executive Order 12333: United States Intelligence Activities	1	[221, 2026]
50.2	Legal Authorities and Constraints - FISA and Surveillance Law	2	[298, 2026]; [297, 2026]
50.3	Legal Authorities and Constraints - Intelligence Community Directives: Full Index (IRP/FAS)	1	[006, 2026]
50.4	Legal Authorities and Constraints - CIA Classification Guide (National Archives)	1	[222, 2026]

Section	Module and source section	Citations	Citation links
50.5	Legal Authorities and Constraints - Allied Legal Frameworks: RIPA, Investigatory Powers Act, GDPR	2	[298, 2026]; [297, 2026]
50.6	Legal Authorities and Constraints - The International Law of Intelligence	2	[298, 2026]; [297, 2026]
51.99	Ethics of Intelligence and Cognitive Security - V2 source-lane extension: bind Ethics of Intelligence and Cognitive Security to source-lane evidence, claim-ledger review, safe substitution, compliance/rights mapping, instructor deliverables, and explicit refresh triggers	3	[238, 2026]; [239, 2026]; [240, 2026]
51.101	Ethics of Intelligence and Cognitive Security - Deep expansion: add accessibility/UDL review, procurement/vendor oversight, HRIA/DPIA worksheet, data-lineage registry, assessment-integrity protocol, agent incident drill, role-based competency map, and adversarial assurance cycle for Ethics of Intelligence and Cognitive Security	3	[278, 2026]; [279, 2026]; [283, 2026]
51.102	Ethics of Intelligence and Cognitive Security - Evidence-package expansion: add model/dataset documentation cards, transparency notice, records-retention audit trail, release/change-control gate, risk-exception memo, learner support plan, instructor question bank, and remediation backlog for Ethics of Intelligence and Cognitive Security	3	[290, 2026]; [291, 2026]; [294, 2026]
51.1	Ethics of Intelligence and Cognitive Security - Intelligence Ethics: Deontological, Consequentialist, Virtue Frameworks	2	[298, 2026]; [297, 2026]
51.2	Ethics of Intelligence and Cognitive Security - The Ethics of Cognitive Security (YorkSpace Dissertation)	1	[172, 2026]
51.3	Ethics of Intelligence and Cognitive Security - AI Ethics in Intelligence: Accountability, Transparency, Proportionality	2	[298, 2026]; [297, 2026]
51.4	Ethics of Intelligence and Cognitive Security - Oversight Mechanisms: Congressional, Inspector General, FISA Court	2	[298, 2026]; [297, 2026]
51.5	Ethics of Intelligence and Cognitive Security - Whistleblowing, Leaking, and the Epistemic Duty of Intelligence Professionals	2	[298, 2026]; [297, 2026]

80.7 Bibliography atlas rows: guide keys, curated anchors, and support-source roles

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[001, 2026]	Epistemic Governance in the Context of Crisis	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	This article examines the concept of epistemic governance during crises.
[002, 2026]	Objectivity	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	ICD 203 directs the heads of IC elements to designate a similar individual or office to respond.
[003, 2026]	Active Inference: Applicability to Different Types of Social	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A 2021 peer-reviewed article by Stephen Fox in the journal Entropy that relates the active inference framework to social organization. It maps concepts such as variational free energy, prediction error, generative models, and Markov blankets onto industrial engineering and quality management practices, treating organizational survival as the maintenance of process control limits.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[004, 2026]	AI Won't Replace Spies—It Will Make Them More Powerful Than Ever	source_guide	reference_guide	reference_guide	reference_guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Tom Mulligan argues that artificial intelligence will enhance rather than replace human intelligence professionals, contending that the future of intelligence lies in human-machine collaboration. He maintains that uniquely human qualities such as intuition, experience, and independent judgment become more valuable as adversaries gain access to the same AI tools.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[005, 2026]	CIA: Studies in AI and Human Intelligence - Semper-Verus	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	A blog post on Semper-Verus summarizing a CIA Studies in Intelligence article, "Espionage in Our AI Future: Why Human Intelligence Still Matters" (Vol. 70, No. 1, March 2026). It argues that as AI makes technical intelligence cheaper and AI-driven fabrication more pervasive, human intelligence becomes relatively more valuable, since human specialists are needed to verify source reliability over time.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[006, 2026]	Director of National Intelligence - Intelligence Community Directives	source_guide_reference_guide	source_guide_reference_guide	source_guide_reference_guide	source_guide_reference_guide_import	source_guide_lifecycle	source_guide_context	bibliography_traceability	source_guide_context	A Federation of American Scientists repository cataloguing the Intelligence Community Directives (ICDs) issued by the Director of National Intelligence. ICDs are the principal means by which the DNI provides policy, guidance, and direction to the U.S. Intelligence Community.
[007, 2026]	THE FRIENDS BRITAIN'S POST-WAR SECRET INTELLIGENCE	source_guide_reference_guide	source_guide_reference_guide	source_guide_reference_guide	source_guide_reference_guide_import	source_guide_lifecycle	source_guide_context	bibliography_traceability	source_guide_context	It is SIS's task to pursue policy objectives by unorthodox means and to amass useful information.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[008, 2026]	Mossad / Military History and Science	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	An EBSCO Research Starter reference article on the Mossad, Israel's national intelligence agency established in 1949 and responsible for foreign intelligence collection and counterterrorism operations conducted outside Israel's borders. It describes the agency's departmental structure (collection, political action and liaison, research, technology) and reviews historically documented operations including the 1960 capture of Adolf Eichmann and the rescue of Ethiopian Jews.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[009, 2026]	“Here to stay” – Chinese state-affiliated hacking for strategic goals	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	A November 2023 report from MERICS (Mercator Institute for China Studies) analyzing Chinese state-affiliated cyber intrusions aimed at strategic goals. It argues that Chinese actors pursue long-term, persistent access to European technology firms and critical infrastructure for espionage rather than disruption, with targeting aligned to government priorities such as semiconductors, pharmaceuticals, and advanced manufacturing.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[010, 2026]	The Five Eyes Archive	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	An online archive maintained by Unredacted UK that compiles declassified government documents on intelligence sharing among the Five Eyes nations (United States, United Kingdom, Canada, Australia, and New Zealand). The collection traces the emergence and evolution of bilateral and multilateral agreements from the postwar era, including the BRUSA and UKUSA agreements, drawing on records from UK, US, and Australian agencies plus freedom-of-information releases.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[011, 2026]	BRUSA and UKUSA Agreements: GCHQ and NSA	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	A curated collection from Unredacted UK presenting documents declassified by the NSA and GCHQ in 2010 relating to US-UK signals intelligence cooperation. It covers the 1946 British-US Communications Agreement (BRUSA), its wartime origins from 1940, and its evolution into the 1956 UKUSA Agreement and the broader Five Eyes alliance.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[012, 2026]	Counterintelligence Activities of Non-State Actors - Grey Dynamics	source guide	reference guide	reference guide	reference guide	source guide lifecycle	source guide context	bibliography traceability	source guide context	A Grey Dynamics analysis article (Rachel Brown, 2021) on how non-state actors conduct counterintelligence. It argues that although such groups lack the technical collection capabilities of states, they compensate through open-source and human-source methods and benefit defensively from compartmentalized, cell-based structures and ideological cohesion.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[013, 2026]	Intelligence Tradecraft Overview / PDF / Surveillance	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	This is an instructional training document hosted on Scribd that introduces the fundamentals of intelligence tradecraft, defined as the methods and skills used in intelligence operations. It covers core concepts and types of tradecraft, cover and operational security, casing and surveillance, clandestine communication, and information gathering.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[014, 2026]	Tradecraft: Covert Operative Tactics and Techniques	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	An educational article from TRD-CRFT defining tradecraft as the techniques, strategies, and tools used by intelligence operatives to pursue objectives while maintaining secrecy and operational security. It surveys core disciplines such as surveillance and counter-surveillance, cover and disguise, technical and human intelligence work, and the field's evolution toward digital and cyber methods.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[015, 2026]	Cover (intelligence gathering)	source_guide_reference_guide_source_guide_reference_guide_source_guide_reference			source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A Wikipedia article explaining the concept of cover in human intelligence and counterintelligence work, defined as the ostensible identity assumed by a covert agent. It distinguishes official cover (diplomatic channels, immunity) from non-official cover (no government acknowledgment, less protection). The article surveys historical examples of front organizations and assumed identities.
[016, 2026]	Surveillance Detection - State.gov	source_guide_reference_guide_source_guide_reference_guide_source_guide_reference			source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Place where victim can be controlled with limited avenues of escape.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[017, 2026]	Language of Espionage / International Spy Museum	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	An educational glossary from the International Spy Museum, a nonprofit institution in Washington, DC, presenting an alphabetized dictionary of espionage terminology. It defines operational roles (agent, handler, case officer), intelligence disciplines such as HUMINT, SIGINT, and IMINT, major organizations (CIA, FBI, KGB, MI5, MI6, NSA), and historical equipment like the Enigma machine and U-2 aircraft.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[018, 2026]	Old-school spycraft could make a comeback as AI undermines trust	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	A Nextgov article reporting on an essay in the CIA's Studies in Intelligence journal by RAND researcher Thomas Mulligan. It argues that as AI makes deepfakes and synthetic communications easier, trust in digital channels erodes, paradoxically increasing the value of traditional human intelligence methods.
[019, 2026]	Espionage in Our AI Future: Why Human Intelligence Still Matters - CSI	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	By Thomas Mulligan, a researcher at the RAND Corporation who served in CIA during 2008–14.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[020, 2026]	The Human Source Management System (Confidential Informant	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A publisher and training-organization page from HSM Training and Consultancy (London) promoting the book The Human Source Management System, a guide of over 500 pages that applies social psychology to the management of confidential informants. The site states the book draws on research and practitioner interviews and is used by law enforcement and intelligence bodies across more than 40 countries.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[021, 2026]	Learn how to be a spy from previously unpublished KGB training	source guide reference guide	reference guide	reference guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A July 2019 story from The World (PRX public radio) about a project led by Michael Weiss to translate previously unpublished Soviet-era KGB training manuals from the 1970s-80s into English. The article describes how the manuals cover intelligence methods such as agent recruitment, psychological manipulation, and disinformation detection, and notes the materials remain relevant because related methods persist in modern Russian services.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[022, 2026]	Summaries of Newly Obtained KGB Training Manuals - The Interpreter	source guide reference	source guide reference	source guide reference	source guide reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	An article from The Interpreter, a publication focused on Russian affairs and disinformation, announcing a project to translate, analyze, and publish previously unpublished Soviet KGB training documents. It summarizes a set of newly obtained manuals spanning several decades and describes the topics they cover, including operational terminology, agent classification, information-gathering methods, recruitment and vetting procedures, and counterintelligence concerns.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[023, 2026]	The Impact of Digital Technology on Clandestine Agent Recruitment	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	A 2024 International Master in Security, Intelligence and Strategic Studies thesis (Glasgow, Trento, Charles University) titled 'Human Intelligence in the Modern Era: The Impact of Digital Technology on Clandestine Agent Recruitment.' It uses a literature-based analysis plus three case studies to compare traditional human-source practices with technology-enabled approaches.
[024, 2026]	Using shared experiences to recruit committed human intelligence	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	Source-guide bibliography entry.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[025, 2026]	Andrew Bustamante: Inside the Mind of a Spy — Tradecraft, Trust	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	This is an episode of The Unmistakable Creative Podcast featuring former CIA field operative Andrew Bustamante discussing intelligence work. The conversation covers his background at the Air Force Academy and CIA training, and frames espionage as resting on reading people, trust, influence, and empathy rather than glamour or action. It also addresses how operatives are selected, the isolation of covert work, and its psychological effects on personal relationships.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[026, 2026]	The tension and drama behind surveillance detection operations	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	A YouTube video titled “Inside the CIA: The tension and drama behind surveillance detection operations,” released May 3, 2024, featuring a former CIA officer. The speaker describes the operational complexity and interpersonal tension involved in moving safely from a starting point to a meeting while accounting for the presence of hostile observation. It conveys the difficulty and stress of clandestine field meetings as recounted from personal experience.
[027, 2026]	The Dead Drop: Design a Communications Method Like a Spy	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	Learn a technique for communicating with your family in an emergency using a method used by spies.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[028, 2026]	Introducing Dead Drops to Network Steganography using ARP-Caches and SNMP-Walks	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	Source-guide bibliography entry.
[029, 2026]	Agent Handling in Counterintelligence / PDF	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	A roughly 28-page Scribd document titled “Agent Handling in Counterintelligence” providing an educational overview of intelligence operations. It surveys the roles of case officers in managing sources, recruitment and training of agents, protective measures such as fronts and cutouts, agent classifications including unwitting sources, and counterintelligence methods for identifying foreign operatives and reducing security breaches.
[030, 2026]	The Secrets of Counter-surveillance	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	Source-guide bibliography entry.
[031, 2026]	KGB counter surveillance: How to know if you’re being followed	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	There are cameras everywhere! Everything is trackable!

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[032, 2026]	TOP SECRET KGB Training Manual - Working with Agents	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	A Google Books catalog entry for a 2025 English-translation edition of a Cold War-era Soviet intelligence training manual, published by Century Print Media Group with a translator's note by a retired NATO intelligence officer. The 144-page volume is presented as a historical document on Soviet human-intelligence doctrine and counterintelligence practice.
[033, 2026]	The Counter-intelligence Threat from Non-State Actors	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	How seriously is the U.S. Intelligence Community (IC) considering this challenge to U.S.
[034, 2026]	Studies in Intelligence Vol. 70, No. 1 (Extracts, March 2026) - CSI	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	Thomas Mulligan is a researcher at the RAND Corporation and former CIA officer. Ana P.
[035, 2026]	Signals Intelligence (SIGINT) Overview	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	SIGINT is intelligence derived from electronic signals and systems used by foreign targets.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[036, 2026]	European Axis Signal Intelligence in World War II	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Volumes 1 - 9 of the European Axis Signal Intelligence in WWII documentation.
[037, 2026]	NSA Releases History of American SIGINT and the Vietnam War	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference import	source guide lifecycle	source guide context	bibliography traceability	source guide context	This Federation of American Scientists article reports on the NSA's declassification of a roughly 500-page historical study titled "Spartans in Darkness," which examines American signals intelligence during the Vietnam War from 1945 to 1975. Author Robert J. Hanyok documents that no second attack occurred during the 1964 Gulf of Tonkin Incident, contradicting prior official testimony, and also covers episodes such as the Tet Offensive and the Son Tay prison rescue.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[038, 2026]	History of signals intelligence at the CIA - Open INT	source_guide_reference_guide_reference_guide_reference_guide_reference	source_guide_reference_guide_reference_guide_reference_guide_reference	source_guide_reference_guide_reference_guide_reference_guide_reference	source guide reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A January 2018 blog post on Open INT recounting the CIA's role in signals intelligence from roughly 1947 to 1970, noting that SIGINT is often associated with the NSA but the CIA also participated. It distinguishes communications intelligence from electronic intelligence and references declassified Cold War operations including U-2 collection and a Berlin communications-tapping effort.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[039, 2026]	The CIA and Signals Intelligence / National Security Archive	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	A 2015 briefing book from the National Security Archive, compiled by Jeffrey T. Richelson, presenting declassified documents on the CIA's signals intelligence activities from roughly 1947 to 1970. It documents the CIA's parallel SIGINT operations alongside the NSA during the Cold War, covering programs and collection efforts as well as recurring friction between the two agencies over mission overlap, budgets, and access to intelligence.
[040, 2026]	BASIC CRYPTOGRAPHY	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	Codes will first be considered, but as they do not fulfill the conditions required of a means.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[041, 2026]	Five Eyes FOIA disclosures	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	A collection page from Unredacted, a UK-based organization focused on declassified government records. It assembles over 70 documents obtained through a 2017 Freedom of Information Act legal challenge led by Privacy International, drawn from US agencies including the NSA, State Department, and Department of Defense.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[042, 2026]	Five Eyes FOIA disclosures: key documents	source_guide	reference_guide	reference_guide	reference_guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A briefing from Unredacted examining previously classified Five Eyes documents released to Privacy International following a 2017 US freedom of information request. The materials, spanning 1945 to 2016, trace the development and functioning of the UKUSA Agreement underpinning intelligence cooperation among the US, UK, Canada, Australia, and New Zealand.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[043, 2026]	Technical Surveillance Countermeasures (TSCM) - Bastille Networks	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	An informational guide from Bastille Networks explaining Technical Surveillance Countermeasures (TSCM), defined as security measures aimed at detecting and neutralizing surveillance devices to protect sensitive communications. It traces TSCM origins to World War II and Cold War intelligence work and catalogues threat types such as radio-frequency transmitters, hidden cameras, and acoustic eavesdropping.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[044, 2026]	Technical Surveillance Threat Levels - Granite Island Group	source_guide_reference	reference_guide_source	reference_guide_source	reference_guide_source	source guide lifecycle	source guide context	bibliography traceability	source guide context	A reference page from the Granite Island Group describing a ten-level taxonomy of technical surveillance threats and the corresponding technical surveillance countermeasures (TSCM) inspections used to detect them. It explains that detection difficulty increases by roughly an order of magnitude at each level, grouping threats into clusters and beginning with low-power consumer-grade devices.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[045, 2026]	TSCM / Technical Surveillance Countermeasures - Pinkerton	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A service page from Pinkerton describing technical surveillance countermeasures used to detect and prevent corporate eavesdropping and protect intellectual property. It outlines examination methods including infrared spectrum analysis to find heat signatures of hidden devices, radio frequency analysis to identify wireless audio bugs, and physical inspection for tampered equipment or poor security practices.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[046, 2026]	The TSCM Inspection Process / by Murray Associates TSCM	source_guide_reference	reference_guide	reference_guide_source	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A web page from Murray Associates, a counterespionage consulting firm, explaining the technical surveillance countermeasures (TSCM) inspection process used to detect eavesdropping and surveillance devices in buildings. It outlines a three-phase methodology: a pre-inspection planning discussion, an on-site evaluation combining visual examination, technical instrumentation, and information-security review, and a post-inspection written report with findings and recommendations.
[047, 2026]	How the Intelligence Community Has Held Back Open-Source	source_guide_reference	reference_guide	reference_guide_source	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Plans and strategies for improving open-source intelligence (OSINT) operations in the Intelligence.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[048, 2026]	The IC OSINT Strategy 2024-2026	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	Tradecraft and training standards must be flexible and updated regularly to keep pace with changes.
[049, 2026]	Open Source Intelligence (OSINT): issues and trends	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	The text explores OSINT's advantages and disadvantages in intelligence activities.
[050, 2026]	Thoughts on Bazzell's New Book? [Open Source Intelligence	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	Mike wrote he wants to make the OSINT investigator more self reliant, able to do his job without.
[051, 2026]	Source-guide chapter: From Recon-ng to Trace Labs – A Tour of the Best Open …	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	Source-guide bibliography entry.
[052, 2026]	What is Open Source Intelligence & Top 10 Tools - Lampyre	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	This article defines open source intelligence as the practice of gathering information from publicly available data for security, business, and investigative purposes, drawing on websites, social media, government records, and public databases.
[053, 2026]	A Guide to Choosing the Right Tool for Your Needs	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	Source-guide bibliography entry.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[054, 2026]	What are your preferred OSINT tools? : r/hacking	source_guide_reference	reference_guide	reference_guide_source	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Recommended OSINT tools and their benefits. Top open source intelligence websites.
[055, 2026]	IntelTechniques Books	source_guide_reference	reference_guide	reference_guide_source	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	OSINT Techniques. Resources for Uncovering Online Information - 11th Edition (2024).
[056, 2026]	IntelTechniques - OSINT 11 2025.04.02 .pdf - el-hacker.INFO	source_guide_reference	reference_guide	reference_guide_source	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	All tutorials in this book were confirmed accurate as of November 1, 2024.
[057, 2026]	MCRP 2-10B.4 (SECURED) - Marines.mil	source_guide_reference	reference_guide	reference_guide_source	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	MCRP 2-10B.4 in the source guide links to the Marines GEOINT manual, not a reconnaissance manual. The linked PDF is 'Geospatial Intelligence Support to Operations'; verify the intended citation before reuse.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[058, 2026]	GEOINT Essential Body of Knowledge	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The GEOINT Essential Body of Knowledge (Version 2.0, 2019), published by the United States Geospatial Intelligence Foundation (USGIF). First developed in 2014 and revised with community input, it defines the competencies, standards, and learning objectives needed to succeed in the geospatial intelligence discipline.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[059, 2026]	neonpangolin/geospatial-intelligence-library	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	A GitHub repository describing itself as a reference toolkit for geolocation and chronolocation in digital investigations. It curates open-source resources organized into categories including satellite imagery, mapping, infrastructure and transport tracking, weather and environmental monitoring, shadow and sun-position tools for time-of-day analysis, crisis and conflict mapping, image forensics, and geocoding utilities.
[060, 2026]	DoDM 3305.10, "DoD Geospatial Intelligence (GEOINT	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	Source-guide bibliography entry.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[061, 2026]	Cyber Kill Chain®	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	This Lockheed Martin webpage describes the Cyber Kill Chain framework, a methodology for identifying and preventing cyber intrusions as part of the company's Intelligence Driven Defense model. It outlines the sequence of steps an adversary must complete to achieve an objective, and is intended to help analysts understand attacker tactics and procedures.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[062, 2026]	Cyber kill chain	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	A Wikipedia article describing the cyber kill chain, a framework adapted by Lockheed Martin from a military concept to model how cyberattacks progress through distinct phases. It outlines seven stages from reconnaissance through actions on objectives, along with defensive countermeasures organizations can apply at each stage.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[063, 2026]	Enterprise Matrix - MITRE ATT&CK®	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The official MITRE ATT&CK Enterprise Matrix, a curated knowledge base of adversary tactics and techniques observed in real-world intrusions. It organizes activity into fifteen sequential tactics, from reconnaissance and resource development through initial access, persistence, privilege escalation, defense evasion, credential access, lateral movement, command and control, exfiltration, and impact.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[064, 2026]	MITRE ATT&CK®	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	MITRE ATT&CK is a globally accessible knowledge base that catalogs adversary tactics and techniques drawn from real-world observations of cyber intrusions. The framework is organized into matrices covering Enterprise, Mobile, and Industrial Control Systems environments, with tactics representing adversary objectives and techniques describing specific methods used to achieve them.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[065, 2026]	Enterprise Techniques - MITRE ATT&CK®	source_guide	reference_guide	reference_guide	reference_guide	source guide lifecycle	source guide context	bibliography traceability	source guide context	The Enterprise Techniques page of the MITRE ATT&CK framework, a cybersecurity knowledge base maintained by MITRE Corporation. It documents 222 enterprise techniques and 475 sub-techniques describing how adversaries achieve tactical goals across the attack lifecycle, organized by tactics such as initial access, persistence, privilege escalation, defense evasion, credential access, discovery, and impact.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[066, 2026]	What is STIX/TAXII? - Cloudflare	source_guide	reference_guide	reference_guide	reference_guide	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A Cloudflare Learning Center explainer describing STIX and TAXII as complementary standards for cyber threat intelligence. STIX defines a structured language for representing threat information, while TAXII specifies how that information is transported and exchanged between systems. Together they form a framework that lets organizations share and consume threat intelligence in a consistent, machine-readable way to improve collective defense.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[067, 2026]	Introduction to STIX	source_guide	reference_guide	reference_guide	reference_guide import	source_guide lifecycle	source_guide context	bibliography traceability	source_guide context	An introductory page from the OASIS CTI documentation explaining STIX (Structured Threat Information Expression), an open-source language and serialization format used to exchange cyber threat intelligence. It describes how STIX 2.1 models intelligence using 18 domain objects (such as attack patterns, malware, threat actors, and vulnerabilities) and 2 relationship objects, all represented as JSON.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[068, 2026]	OASIS Cyber Threat Intelligence (CTI) TC	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	bibliography traceability	source_guide_reference	The official committee page for the OASIS Cyber Threat Intelligence (CTI) Technical Committee, a standards body that develops formats for sharing cyber threat intelligence. It maintains the STIX (Structured Threat Information Expression) data model and the TAXII exchange protocol, both approved as OASIS standards in 2021, and organizes subcommittees for STIX, TAXII, and interoperability.
[069, 2026]	Assessing nation-state-sponsored cyberattacks using aspects	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	bibliography traceability	source_guide_reference	They found that the most common cyberattacks initiated by nation-states were espionage focused.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[070, 2026]	Getting Harder to Catch Analyzing the Evolution of China's Cyber	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	A 2016 student security paper by Winnona DeSombre (Tufts Comp116) analyzing the evolution of China's cyber espionage campaigns against the United States. Organized in three parts, it surveys China-US relations in the cyber domain and the policy dilemmas of attribution and shared terminology, presents a case study of the APT1 hacker group linked to PLA Unit 61398, and reviews broader trends in the context of the 2015 US-China Cyber Agreement.
[071, 2026]	I Led IR on Nation-State Attacks at Mandiant, FireEye & CrowdStrike	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	Attribution becomes harder when its open-source …
[072, 2026]	ATT&CK-based Advanced Persistent Threat attacks risk propagation	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	The Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework introduced.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[073, 2026]	SolarWinds Supply Chain Attack - Fortinet	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference import	source guide lifecycle	source guide context	bibliography traceability	source guide context	This Fortinet cybersecurity glossary page provides educational material about the SolarWinds supply chain attack. It explains how attackers compromised SolarWinds' Orion monitoring software with malicious code that spread to roughly 18,000 customers through software updates beginning in early 2020, and notes the attack's extended timeline and impact on U.S. federal agencies and major companies.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[074, 2026]	How to Protect Against a Supply Chain Compromise - Vectra AI	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A Vectra AI blog post from April 2024 analyzing the XZ Utils backdoor, a malicious commit discovered on March 29, 2024 in a widely used open-source compression library that could compromise affected systems via SSH. The article frames the incident as a supply chain compromise affecting both open-source and commercial software, drawing comparison to SolarWinds.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[075, 2026]	The Xz-Utils Backdoor: The Supply Chain RCE That Got Caught	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	An Invicti Security blog post from April 2024 analyzing the xz-utils backdoor, a software supply chain compromise discovered in versions 5.6.0 and 5.6.1 of the compression library. It describes how malicious code was hidden in test files and assembled only during compilation, potentially enabling unauthenticated remote code execution via OpenSSH, and how a long-term contributor gradually gained maintainer trust before inserting it.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[076, 2026]	XZ Utils backdoor	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	In early 2024, a malicious backdoor was discovered embedded in XZ Utils, a widely used compression library in Linux distributions, designed to enable unauthorized remote code execution via OpenSSH using an Ed448 private key. The perpetrator, operating under the pseudonym Jia Tan, spent over two years building trust as a contributor before inserting the exploit, which received a maximum CVSS score of 10.0.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[077, 2026]	An Evidence-Driven Analysis of Threat Information Sharing	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	An arXiv research paper presenting an evidence-driven analysis of why threat information sharing for industrial control systems remains ineffective. Drawing on three major ICS attacks and a review of 196 procedure examples across 22 malware families, it identifies limitations including incomplete support in the STIX sharing standard, reliance on proprietary undocumented protocols, and insufficient technical detail in threat and vulnerability reports.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[078, 2026]	Advanced Criminal Investigations and Intelligence Operations: Tradecraft Methods, Practices, Tactics, and Techniques/Paperback	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A Barnes & Noble listing for Advanced Criminal Investigations and Intelligence Operations by Robert J. Girod. The book examines tradecraft, defined as the methods, practices, and techniques used in espionage and clandestine investigations.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[079, 2026]	Financial intelligence	source_guide_reference_guide_source_reference_guide_source_reference_guide_source_reference_guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The Wikipedia article on financial intelligence (FININT), defined as gathering information about the financial affairs of entities of interest to understand their nature, capabilities, and intentions. It outlines two core components: collection, in which Financial Intelligence Units gather transaction data and suspicious activity reports from banks, and analysis, in which specialists use data mining to detect tax evasion, money laundering, and terrorist financing.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[080, 2026]	Financial intelligence	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A Wikipedia article on financial intelligence (FININT), the gathering and analysis of information about financial transactions to detect illicit activity such as money laundering, tax evasion, and terrorist financing. It distinguishes two core functions: collection of raw transaction data and suspicious activity reports by government financial intelligence units, and analysis using data-matching techniques to identify suspicious patterns. The article describes the U.S.
[081, 2026]	Financial intelligence	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The Citizendium 'Financial intelligence' article was never written; the page is empty. Use an authoritative alternative source for financial intelligence definitions.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[082, 2026]	Financial Intelligence: A Crucial Pillar of National Security	source_guide	reference_guide	reference_guide	reference_guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A 2025 article by Kevin Hk Chow in Modern Economy titled “Financial Intelligence: A Crucial Pillar of National Security.” It argues that Financial Intelligence (FININT) serves as a critical interface between economic systems and national security, used to detect and disrupt illicit financial networks tied to money laundering, terrorism financing, and transnational crime.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[083, 2026]	JP 3-53, “Doctrine for Joint Psychological Operations”	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Joint Publication 3-53, the US Department of Defense joint doctrine for psychological operations. It establishes organizational structure, command relationships, planning processes, and approval authorities for integrating psychological operations into joint military campaigns and peacetime activities.
[084, 2026]	JP 3-53 Doctrine for Joint Psychological Operations	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Joint Publication 3-53, Doctrine for Joint Psychological Operations (Joint Chiefs of Staff, 10 July 1996). This US military doctrine document establishes the doctrinal basis for planning and conducting psychological operations in support of joint military operations.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[085, 2026]	Military Information Support Operations	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference import	source guide lifecycle	source guide context	bibliography traceability	source guide context	It sets forth joint doctrine to govern the activities and performance of the Armed Forces.
[086, 2026]	Tactical Psychological Operations Manual / PDF / Computers	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A U.S. military field manual, FM 3-05.302, providing doctrine for tactical psychological operations at the unit level. The roughly 255-page document covers the organization of these units, command relationships when supporting joint forces, a multi-phase product development and assessment process, and how intelligence supports such operations. It serves as a comprehensive training and reference document for personnel involved in tactical influence operations.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[087, 2026]	FM 3-05.301 Psychological Operations Process Tactics, Techniques	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	…
[088, 2026]	SOVIET ‘ACTIVE MEASURES’ FORGERY, DISINFORMATION, POLITICAL OPERATIONS	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A U.S. Department of State Bureau of Public Affairs report from October 1981, released under FOIA. It catalogs Soviet ‘active measures’ — the Soviet term for covert influence operations — including written disinformation, control of foreign media, use of front organizations, clandestine broadcasting, blackmail, and political influence operations. Specific cases include Soviet forgeries related to the 1979 Grand Mosque seizure and NATO theater nuclear force debates.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[089, 2026]	SOVIET ACTIVE MEASURES AND DISINFORMATION: OVERVIEW AND ASSESSMENT	source_guide_reference_guide_source_guide_reference_guide_source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	An article by Dennis Kux published in Parameters: Journal of the US Army War College (1985) and preserved in the CIA CREST archive. It defines and distinguishes Soviet 'disinformation' and 'active measures,' situating them within a spectrum of white, gray, and black foreign influence operations. Kux examines KGB front groups, agents of influence, forgeries, and the broader strategic goal of tarnishing Western governments while advancing Soviet foreign policy.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[090, 2026]	“SOVIET ACTIVE MEASURES: FORGERY, DISINFORMATION, POLITICAL OPERATIONS”	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A CIA CREST record (October 1981, released March 2007) comprising a routing and record sheet from the PCS/PGLO office dated February 8, 1982, attached to the same Department of State Special Report No. 88 on Soviet active measures. The document is catalogued as an open-source CREST entry and captures the internal CIA circulation of the State Department’s public report on Soviet forgery and disinformation operations.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[091, 2026]	SOVIET ACTIVE MEASURES AND DISINFORMATION	source_guide	reference_guide	reference_guide	reference_guide	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A declassified-in-part 1986 CIA speech text on Soviet active measures, prepared by the Foreign Activities Branch, Third World Activities Division, Office of Soviet Analysis. It explains the KGB's use of forgeries, disinformation, and front organizations to covertly influence foreign governments and publics, illustrating with the forged 1984 Olympic KKK leaflet operation designed to discourage participation in the Los Angeles Games.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[092, 2026]	INTRODUCTION	source guide	reference guide	reference guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A March 2019 CREST (Centre for Research and Evidence on Security Threats) report titled “Russia and Disinformation: Maskirovka,” prepared by scholars of Russian foreign and security policy using open-source and Russian-language primary material. It examines the historical background of Soviet and Russian disinformation, including the concept of active measures, and how disinformation is woven into strategic narratives and diplomacy.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[093, 2026]	Deception, Disinformation, and Strategic Communications	source_guide	reference_guide	reference_guide	reference_guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Fletcher Schoen and Christopher J. Lamb, 'Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference,' INSS Strategic Perspectives No. 11 (NDU Press, June 2012). The study examines the U.S. Active Measures Working Group, a small interagency committee formed in the 1980s to expose and counter Soviet disinformation, and analyzes why it succeeded where most such groups fail.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[094, 2026]	Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	Fletcher Schoen and Christopher J. Lamb, 'Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference,' INSS Strategic Perspectives No. 11 (NDU Press, June 2012).
[095, 2026]	COGNITIVE SECURITY IN THE AGE OF AI	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	This policy paper examines the emergence of cognitive security.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[096, 2026]	AI DEVELOPMENT SHOULD PRIORITIZE COGNITIVE SECURITY	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	A position paper (Stanford authors, ICLR 2026 workshop) arguing that AI research and development should prioritize cognitive security, defined as protecting human cognitive processes from hazardous influence. It notes that generative AI systems increasingly designed to influence beliefs and behavior raise acute governance concerns, while research on these effects remains fragmented.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[097, 2026]	The History of Social Engineering	source_guide	reference_guide	reference_guide	reference_guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	This Mitnick Security guide traces the history and evolution of social engineering from antiquity through modern cyberattacks. It surveys major attack categories including phishing and its variants, pretexting, baiting, tailgating, and quid pro quo schemes, and explains the psychological influence principles such as reciprocity, scarcity, authority, and consensus that attackers exploit.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[098, 2026]	Social Engineering: T he Science of Human Hacking	source_guide	reference_guide	reference_guide	reference_guide	source guide lifecycle	source guide context	bibliography traceability	source guide context	The full text of “Social Engineering: The Science of Human Hacking” (2nd edition, 2018) by Christopher Hadnagy, published by John Wiley & Sons. The book examines the human element of security, analyzing how manipulation and persuasion techniques can be used to influence people, and how individuals and organizations can recognize and defend against such tactics. It is written as a professional reference on understanding and countering human-targeted security threats.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[099, 2026]	Social Engineering: The Art of Human Hacking	source guide reference	reference guide	reference guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A PDF of the book Social Engineering: The Art of Human Hacking by Christopher Hadnagy, a foundational security text on how attackers exploit human psychology rather than technical flaws to obtain information or access. The work surveys manipulation tactics and the human factors that make organizations vulnerable, and frames this knowledge defensively to help security professionals recognize and resist such attacks.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[100, 2026]	A Survey on Large Language Model-based Agents in Autonomous	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	This survey examines how large language model-based agents can be weaponized as autonomous cyberattack tools, analyzing their architecture across five core components: models, perception, memory, reasoning and planning, and tools. The authors document eight attack categories and map them across static infrastructure, mobile networks, and infrastructure-free systems such as blockchain and the metaverse.
[101, 2026]	Information Warfare: An Air Force Policy for the Role of Public Affairs	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The military's use or misuse of information in psychological or deception operations, under.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[102, 2026]	Information Warfare and Deception	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A 2006 paper by William Hutchinson published in the journal Informing Science. It examines the history of information warfare and the increasingly central role of deception within it, tracing the concept from its late-1980s origins as a technology-oriented military tactic for command-and-control dominance to a broader recognition of information itself as both weapon and target.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[103, 2026]	Military Deception	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A topic page from the Journal of Information Warfare collecting scholarly articles on military deception. Featured pieces argue that information operations officers should be conceptualized primarily as deception officers, and one quantitative reassessment reports that deception is employed in roughly 30 to 53 percent of military operations.
[104, 2026]	The Utility of Military Deception and Information Operations	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference import	source guide lifecycle	source guide context	bibliography traceability	source guide context	An essay published in Small Wars Journal (June 2025) by a U.S. Army Civil Affairs officer arguing that military deception and information operations have become central to modern conflict.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[105, 2026]	Automated influence and the challenge of cognitive security	source guide reference	source guide reference	source guide reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Sarah Rajtmajer and Daniel Susser, 'Automated Influence and the Challenge of Cognitive Security,' in Hot Topics in the Science of Security (HotSoS '20), April 2020, ACM. The paper argues that AI-powered computational propaganda poses national security threats that existing ethical frameworks do not address, and proposes 'cognitive security' as a productive conceptual lens for evaluating the ethics of automated influence operations and potential defensive responses.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[106, 2026]	Applications of The Active Inference and The Free-Energy Principle	source guide	source guide	source guide	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A 2024 bachelor's thesis by Lara Sakarya at Delft University of Technology presenting a systematic literature review of the active inference framework and the free-energy principle as applied to mimicking social human behavior in intelligent agents. It explains active inference as a theory describing behavior that minimizes surprise, and surveys model variants such as deep active inference, multi-modal deep belief networks, predictive coding, and probabilistic programming.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[107, 2026]	Behavioral Outcomes of Human Cognitive Security	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	An arXiv research paper (March 2026) proposing an integrative modeling framework for human cognitive security, defined as the degree to which people rely on truthful information to make truth-aligned judgments. It synthesizes Bayesian belief-updating with Prospect Theory to model how cognitive resources and emotional valuation shape behavior, and identifies three observable outcomes: veracity discernment, task-oriented actions, and information sharing.
[108, 2026]	Critical Thinking techniques	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A Tradecraft Primer: Structured Analytic Techniques for Improving. Intelligence Analysis.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[109, 2026]	The ‘Grey Zone’ and Hybrid Activities	source guide reference	source guide reference	source guide reference	source guide reference import	source guide lifecycle	source guide context	bibliography traceability	source guide context	This is a peer-reviewed article in Connections: The Quarterly Journal (Vol. 21, No. 2, Spring 2022) by Peter Dobias and Kyle Christensen examining military competition below the threshold of armed conflict. It analyzes how Russia, China, and Iran operate in the space between peace and war, describing Russia’s emphasis on information measures, China’s maritime and force approaches, and Iran’s anti-access and proxy strategies.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[110, 2026]	A Full Spectrum of Conflict Design: How Doctrine Should Embrace	source_guide	reference_guide	reference_guide	reference_guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	An article by Dr. Robert S. Burrell on the Irregular Warfare Initiative arguing that U.S. military doctrine inadequately addresses gray zone and hybrid warfare. It proposes a two-dimensional framework spanning peace-to-war and direct-to-indirect means, yielding four approaches: traditional warfare, deterrence, irregular warfare, and competition.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[111, 2026]	Anonymous No More: Countering the Gray Zone Threat - from MIPB	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	An article in the U.S. Army's Military Intelligence Professional Bulletin on countering gray zone threats. It discusses how adversaries operate below the threshold of open conflict using hybrid activities across tactical, operational, and strategic levels, and considers how military intelligence can identify and attribute actors who attempt to remain anonymous. The piece is framed around adapting intelligence practice to contemporary competition short of war.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[112, 2026]	Full text of “Special Forces Unconventional Warfare”	source_guide	reference_guide	reference_guide	reference_guide import	source_guide lifecycle	source_guide context	bibliography traceability	source_guide context	This U.S. Army Training Circular (TC 18-01) defines the Special Forces concept for planning and conducting unconventional warfare operations, covering how units enable and support resistance movements in denied or hostile territory. It presents a seven-phase operational framework encompassing psychological preparation, infiltration, organization of underground and guerrilla forces, employment, and transition.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[113, 2026]	FM 3-05.130 Army Special Operations Forces Unconventional	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	U.S. Army Field Manual FM 3-05.130, "Army Special Operations Forces Unconventional Warfare," published by Headquarters, Department of the Army in September 2008. The manual is organized into chapters covering an introduction to warfare types, the instruments of United States national power, national policy and doctrine, and planning considerations including the seven phases of unconventional warfare and the role of Army Special Operations Forces.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[114, 2026]	Army Special Operations Forces Unconventional Warfare	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	FM 3-05.130, Army Special Operations Forces Unconventional Warfare (Headquarters, Department of the Army, 30 September 2008). The manual defines unconventional warfare and situates it within U.S. national power, covering the seven phases of UW operations, Special Forces missions, psychological operations, civil affairs operations in the UW context, and the roles of supporting elements including interagency partners. Distribution was restricted to U.S.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[115, 2026]	Army Special Operations Forces Intelligence	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	FM 3-05.102, Army Special Operations Forces Intelligence (Headquarters, Department of the Army). The manual addresses intelligence and electronic warfare (IEW) support across Army Special Operations Force components, covering Special Forces, Rangers, ARSOA, PSYOP, and Civil Affairs operations.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[116, 2026]	Army Special Operations Forces Intelligence	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	A U.S. Army field manual, FM 3-05.102 (Army Special Operations Forces Intelligence), dated 2001 and superseding FM 34-36, distributed with restrictions to U.S. government agencies. The manual gives special operations forces commanders and staff a doctrinal overview of intelligence support to their missions, covering force structure, training, and operational requirements consistent with joint doctrine.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[117, 2026]	Office of Strategic Services (OSS) Manuals	source_guide	reference_guide	reference_guide	reference_guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	An article from Small Wars Journal (affiliated with Arizona State University) announcing that The Resistance Hub has compiled declassified Office of Strategic Services (OSS) manuals for public access. The OSS was the WWII predecessor to the CIA, and the documents illustrate how the United States organized clandestine activities in occupied Europe and Asia.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[118, 2026]	Special Operations Field Manual, Strategic Services (provisional	source_guide_reference_guide_source_guide_reference_guide_source_guide_reference			source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A digitized World War II field manual from the Internet Archive, the Special Operations Field Manual, Strategic Services (provisional), issued July 18, 1944 by the U.S. Office of Strategic Services (OSS). The 32-page manual sets out the authorized functions, operational plans, methods, and organization of OSS Maritime Units and the broader Special Operations Branch.
[119, 2026]	office of strategic services - ARSOF History	source_guide_reference_guide_source_guide_reference_guide_source_guide_reference			source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Source-guide bibliography entry.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[120, 2026]	PRINCIPLES OF TRADECRAFT	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Principles of Tradecraft, a 1995 publication by Militia Free Press (a subsidiary of The Resister). The document presents an overview of intelligence and espionage concepts, with chapters covering an introduction to espionage, agents (typology, identification, recruitment, and handling), and agent organization and management including personnel and structures. It is framed as an introductory treatment rather than a comprehensive reference on intelligence requirements.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[121, 2026]	How the KGB handled information - Blockint	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference import	source guide lifecycle	source guide context	bibliography traceability	source guide context	This is a Blockint blog post by Ludo Block, published in October 2022, analyzing a KGB training manual on information handling released by the Free Russia Foundation. The manual, written for foreign intelligence officers, sets out six requirements for valuable intelligence and a framework for evaluating sources based on past performance and competence.
[122, 2026]	The Lubyanka Files - Free Russia Foundation THINK TANK	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Source-guide bibliography entry.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[123, 2026]	Full text of “KGB Alpha Team Training Manual” - Internet Archive	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	A 1993 Paladin Press publication presenting a translated Soviet special-operations training text attributed to A. I. Dolmatov, accompanied by an extensive preface by Western trainer Jim Shortt. The preface traces the evolution of Soviet special forces from the 1917 revolution through the Cold War and describes organizations such as the KGB, MVD, and GRU and units including Alpha, Spetsnaz, and OMON.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[124, 2026]	The Logician (The Zinoviev's case). Folder 46. The Chekist	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	This article draws on the Mitrokhin Archive, compiled by defected KGB archivist Vasili Mitrokhin, to document Soviet state surveillance of dissident philosopher Alexander Zinoviev, who was assigned the codename Logician by the KGB's Fifth Chief Directorate. Zinoviev faced professional retaliation including revocation of his doctorate and expulsion from the Communist Party following the publication of satirical anti-Soviet works such as Yawning Heights.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[125, 2026]	Mitrokhin Archive	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The Wilson Center Digital Archive link for the Mitrokhin Archive is a dead staging domain. The Mitrokhin Archive documents Soviet KGB history; use the published Cambridge University Press edition or Wilson Center production archive instead.
[126, 2026]	Mitrokhin Archive	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A Wikipedia article on the Mitrokhin Archive, a collection of hand-written notes made by KGB archivist Vasili Mitrokhin documenting Soviet intelligence operations from the 1930s through the 1980s. Mitrokhin secretly copied files between 1972 and 1984 while overseeing the relocation of KGB foreign intelligence archives, and after the Soviet collapse defected to the UK in 1992 with the material.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[127, 2026]	The Mitrokhin archive : the KGB and the world	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	An Internet Archive record for The Mitrokhin Archive: The KGB and the World, a two-volume work by Christopher Andrew published in 1999 by Allen Lane, running to roughly 1,050 pages. The volumes draw on materials compiled by former KGB officer Vasili Mitrokhin to document Soviet intelligence operations, with the first volume covering the KGB in Europe and the West and the second addressing the KGB and the wider world.
[128, 2026]	Full text of “The Secret War The Office of Strategic Services in World	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	An Internet Archive full-text scan of the proceedings of a 1991 National Archives conference on the Office of Strategic Services (OSS), the U.S.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[129, 2026]	OSS Resources - Office of Strategic Services Society	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A resource directory page from the Office of Strategic Services Society, a historical organization dedicated to preserving the record of the WWII-era OSS. The page functions as a curated library of links to external sites covering OSS history, including operations, related organizations, notable figures such as William Donovan and Allen Dulles, educational materials, and geographic theaters.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[130, 2026]	The Official CIA Manual of Trickery and Deception	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	A reproduction of a Cold War-era manual written by magician John Mulholland for the CIA, presented with commentary by H. Keith Melton and Robert Wallace as "The Official CIA Manual of Trickery and Deception." The book situates the manual within the history of the MKULTRA program and the long-missing magic manuals, and reproduces Mulholland's guidance on applying sleight-of-hand and misdirection techniques to covert operational tasks.
[131, 2026]	Center for the Study of Intelligence - CSI	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	The Center for the Study of Intelligence (CSI) serves as a producer and repository of unclassified.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[132, 2026]	Studies in Intelligence	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Studies in Intelligence is the CIA's professional journal, published by the Center for the Study of Intelligence (CSI). It covers historical, analytical, and methodological topics across the intelligence profession, and is issued quarterly in partially declassified extract form. As of 2026 the archive holds 110 issues, with the most recent being Volume 70, No. 1 (March 2026); articles are written by intelligence community professionals under their own names or pen names.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[133, 2026]	Studies in Intelligence: New Articles from The CIA's In-House Journal	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	This is a National Security Archive briefing book presenting declassified articles from the CIA's internal journal Studies in Intelligence, first published in 1955. The collection gathers articles obtained through Freedom of Information Act requests and litigation, spanning CIA history from the Kennedy era through the post-9/11 period.
[134, 2026]	What is your reading list for (counter)intelligence/tradecraft?	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	How To Be A Spy: The WW2 SOE Training Manual - Denis Rigden · The CIA Guide to Clandestine.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[135, 2026]	The origins of the UKUSA Agreement	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	A briefing from Unredacted, a UK investigative outlet, covering the early development of the UKUSA Agreement, the postwar US-UK signals-intelligence framework that became the basis for the Five Eyes alliance. It traces the 1946 BRUSA agreement on intelligence exchange, Canada's negotiation toward equal partnership in 1949, and the gradual integration of Australia and New Zealand through the 1950s.
[136, 2026]	Mossad's secretive operations and reputation - Facebook	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	The Mossad is concerned with foreign intelligence gathering, intelligence analysis.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[137, 2026]	[2601.12560] Agentic Artificial Intelligence (AI)	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	An arXiv paper surveying the shift from passive language models to Agentic AI, where large language models act as cognitive controllers that combine memory, tool use, and environmental feedback to pursue extended goals. It proposes a unified taxonomy organizing agent systems into six components: perception, brain, planning, action, tool use, and collaboration.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[138, 2026]	Agentic Artificial Intelligence (AI): Architectures, Taxonomies	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	An arXiv survey paper on agentic AI examining the shift from generative systems to autonomous agents that perceive, reason, plan, and act. It proposes a unified taxonomy decomposing LLM-based agents into six dimensions: core components, cognitive architecture, learning paradigms, multi-agent systems, environments and domains, and evaluation and safety.
[139, 2026]	Agentic AI Design Patterns by Andrew Ng	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A LinkedIn post by Aishwarya Srinivasan discussing agentic AI design patterns for building production-grade AI agents.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[140, 2026]	The agentic AI landscape and its conceptual foundations	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	An OECD Artificial Intelligence Paper (No. 56, February 2026) titled "The Agentic AI Landscape and Its Conceptual Foundations," prepared by OECD staff with an expert group.
[141, 2026]	Agentic AI, explained	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	An MIT Sloan explainer article on agentic AI, defining autonomous software systems that perceive, reason, and act to complete multi-step tasks with minimal human intervention. It distinguishes such agents from chatbots, cites a 2025 MIT Sloan/BCG survey finding 35% of companies had deployed agents with 44% planning to, and reviews business applications such as fraud detection and customer service.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[142, 2026]	Agentic AI: A Comprehensive Survey of Architectures, Applications	source guide reference	reference guide	reference guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The arXiv abstract page for "Agentic AI: A Comprehensive Survey of Architectures, Applications," a 2025 paper by Mohamad Abou Ali and Fadi Dornaika. Based on a PRISMA systematic review of roughly 90 studies from 2018 to 2025, it proposes a dual-paradigm framework distinguishing symbolic/classical systems based on algorithmic planning and persistent state from neural/generative systems driven by stochastic generation and prompt orchestration.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[143, 2026]	Agentic AI Architectures And Design Patterns / by Anil Jain	source_guide	reference_guide	reference_guide	reference_guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A Medium article by Anil Jain (2025) surveying agentic AI system architectures and design patterns. It defines agentic AI as systems capable of independent decision-making, reviews frameworks such as LangChain, LlamaIndex, and AutoGen, and describes five system components: perception, decision-making, action, memory, and communication.
[144, 2026]	Agentic AI patterns and workflows on AWS	source_guide	reference_guide	reference_guide	reference_guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	An AWS Prescriptive Guidance document (July 2025) introducing agentic AI patterns and workflows. It presents reusable design templates for building AI agent systems that operate with autonomy while remaining controllable and aligned with goals, aimed at architects, developers, and product leaders.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[145, 2026]	A Scalable Design Pattern for Agentic AI Systems	source_guide	reference_guide	reference_guide	reference_guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	This is an arXiv research paper by Sivasathivel Kandasamy titled “Control Plane as a Tool: A Scalable Design Pattern for Agentic AI Systems.” It proposes an architectural pattern in which AI agents interact with a single control-plane interface that handles tool routing and selection, rather than exposing many tools directly.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[146, 2026]	Agentic AI Frameworks: Key Components & Top 8 Options in 2026	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	An Exabeam explainer describing agentic AI frameworks as software toolkits that provide pre-built components and architectures for building autonomous AI agents. It outlines core elements such as agent coordination, tool integration, memory management, workflow definition, and deployment monitoring, and reviews eight frameworks including LangGraph, AutoGen, CrewAI, LlamaIndex, Haystack, DSPy, and Semantic Kernel.
[147, 2026]	Agent Framework Security	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Security analysis of major AI agent frameworks including LangChain, CrewAI, AutoGen, Semantic.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[148, 2026]	How Riverside Research Advances Agentic AI for National Security	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	This article by Riverside Research traces AI's evolution from large language models through retrieval-augmented systems, single-task agents, collaborative agentic systems, and toward emergent multi-agent autonomy capable of managing surveillance and decision support at operational speed.
[149, 2026]	What is Agentic AI in Security Operations? Autonomous SOC Agents …	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	A 2025 blog article from Simbian AI explaining the application of agentic AI to security operations centers. It describes an architecture organized into perception, cognitive, and action modules, and a coordinated framework of specialized agents for tasks such as alert triage, threat investigation, and vulnerability management.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[150, 2026]	The Right Role for Agentic AI in Security Operations	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	An article from Cybersecurity Tribe examining where autonomous AI should and should not operate within security operations, drawing on survey data and commentary from numerous security experts. It identifies high-volume, repetitive tasks such as alert triage and policy validation as well suited to automation, while warning against autonomous handling of irreversible or high-impact decisions affecting infrastructure and access.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[151, 2026]	A Practical Guide to Prebunking Misinformation - Inoculation Science	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A practitioner guide from Inoculation Science explaining prebunking as a proactive strategy to build preemptive resilience to misinformation. Grounded in inoculation theory, it describes how exposing people to weakened forms of manipulative content can help them develop resistance before they encounter it in the wild.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[152, 2026]	Social media experiment reveals potential to 'inoculate' millions	source_guide_reference	reference_guide	reference_guide	reference_guide_import	source_guide_lifecycle	source_guide_context	bibliography_traceability	source_guide_context	A University of Cambridge news article describing a large study, conducted with Bristol University and Google's Jigsaw, testing whether short animated videos can help people resist online manipulation. The 90-second clips expose common manipulation techniques such as scapegoating, false dichotomies, and emotionally manipulative language, an approach the researchers call prebunking.
[153, 2026]	Agentic AI is exploding, but which framework should you bet on?	source_guide_reference	reference_guide	reference_guide	reference_guide_import	source_guide_lifecycle	source_guide_context	bibliography_traceability	source_guide_context	The second half of the framework highlights common agentic frameworks.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[154, 2026]	CrewAI	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The homepage of CrewAI, a commercial platform for building, deploying, and managing AI agents at scale for enterprises. It presents the product as covering the full lifecycle from identifying automation opportunities to launching and optimizing multi-agent workflows while maintaining enterprise-level control.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[155, 2026]	Model Context Protocol (MCP): Security Design Considerations	source_guide_reference_guide_source_reference_guide_source_reference_guide_source_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	Radosevich and Halloran (2025) audit security vulnerabilities in Anthropic's Model Context Protocol (MCP), which allows LLMs to integrate with external tools and data sources. The authors demonstrate that language models using MCP can be manipulated through prompt injection to execute malicious code, enable remote access, and steal credentials.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[156, 2026]	MCP Security 101: A New Protocol for Agentic AI - Protect AI	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A Protect AI blog post (April 2025) introducing the Model Context Protocol (MCP), the open-source layer Anthropic introduced in November 2024 to standardize how large language model applications connect to data sources and tools. The article explains how MCP acts as middleware between models and downstream services and surveys associated security risks, including overly broad permissions, unvetted servers, exposed endpoints, and limited monitoring.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[157, 2026]	Building Agentic AI with MCP - Bandwidth	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	This is a Bandwidth blog post explaining how the Model Context Protocol (MCP) supports agentic AI systems that can assess context and take actions rather than only respond to prompts. Using a contact-center voice agent example, it describes MCP as a standard for letting AI models interact securely with external tools, APIs, and data sources, and covers instructions versus multi-step workflows.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[158, 2026]	AI Spotlight: MCP (Model Context Protocol) and Agentic AI systems	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A Gravitee blog post explaining the Model Context Protocol (MCP), an open standard developed by Anthropic for how applications provide context and tools to large language models. It compares MCP to a universal connector that replaces custom per-tool integrations, describing an architecture of hosts, clients, and servers and benefits such as reusability, provider flexibility, and improved access controls. The post situates MCP within the broader growth of agentic AI systems.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[159, 2026]	Security Risks of Agentic AI: A Model Context Protocol (MCP	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A September 2025 Bitdefender Business Insights article by Martin Zugec examining security risks in the Model Context Protocol, the standard introduced by Anthropic for connecting AI agents to external tools and data. It identifies concerns including weak default authentication, supply-chain exposure from compromised tools, over-permissioned access tokens, injection and context-poisoning attacks, and gaps in audit logging for agentic workflows.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[160, 2026]	Breaking down the Top 12 Papers on Agentic AI Governance	source guide reference	reference guide	reference guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Oliver Patel compiled a three-part series summarizing twelve influential research papers on governing autonomous AI systems, organized around themes of security and safety, infrastructure and principal-agent theory, and regulatory and capability assessment. The papers collectively argue that governance cannot be applied reactively after agents act but must instead be embedded at the architectural level, preventing unauthorized autonomous behavior before it occurs.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[161, 2026]	New Governance Frameworks Offer a Roadmap for Managing Risks	source_guide	reference_guide	reference_guide	reference_guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A January 2026 article from the law firm Davis Wright Tremaine on governance frameworks for agentic AI. It argues that autonomous, adaptive AI systems pose distinct risks, such as unauthorized or erroneous actions, biased decisions, data breaches, and opaque audit trails, that require governance beyond existing AI frameworks.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[162, 2026]	Agentic AI report reveals need for reliable autonomous operations	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A Dynatrace blog post summarizing its Pulse of Agentic AI 2026 report, based on a survey of over 900 organizational leaders on enterprise adoption of agentic AI. It finds high adoption in IT operations alongside planned budget increases, while identifying barriers to scaling including security and compliance concerns, difficulty monitoring agents, and unclear autonomy boundaries.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[163, 2026]	Karl Friston's Groundbreaking Research Lays the Foundation	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	An article on denise-holt.us covering a 2024 paper by VERSES AI researchers, led by Mahault Albarracin and co-authored by Karl Friston, titled Shared Protentions in Multi-Agent Active Inference. It explains how intelligent agents can develop shared, mutually aligned expectations about future states that enable coordinated group behavior without explicit communication, drawing on Husserl's work on temporal consciousness.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[164, 2026]	VERSES to Present Research at Active Inference Workshop	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A press release from VERSES AI (August 2024) announcing that the company would act as lead sponsor of and present research at the 5th International Workshop on Active Inference (IWAI 2024) in Oxford. It states that VERSES researchers had 12 accepted papers spanning foundational capabilities, multi-agent systems, applications, and ethics, and that the company's chief scientist Karl Friston would speak.
[165, 2026]	Unveiling the multi-faceted concept of cognitive security	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	We provide a comprehensive review of the current state of cognitive security.
[166, 2026]	Defining comprehensive cognitive security in the digital era: Literature review and concept analysis	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Cognitive security, as an emerging field.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[167, 2026]	Unveiling the multi-faceted concept of cognitive security	source guide reference	source guide reference	source guide reference	source guide reference import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A LinkedIn post by Fran Casino announcing a research article titled 'Unveiling the multi-faceted concept of cognitive security: Trends, perspectives, and future challenges,' published in the Elsevier journal Technology in Society. The post describes the work as a literature review that analyzes definitions, challenges, and future trends in cognitive security and proposes a redefinition based on the concept's core components.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[168, 2026]	DARPA Seeks Proposals For Intrinsic Cognitive Security Program	source_guide	reference_guide	reference_guide	reference_guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A Potomac Officers Club news article reporting on a DARPA request for proposals under its Intrinsic Cognitive Security program. The program seeks to protect mixed reality devices from cognitive attacks using mathematical approaches called formal methods, addressing risks such as flooding a device with information to induce motion sickness, distraction, or false alarms.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[169, 2026]	ICS / DARPA	source_guide_reference_guide_source_guide_reference_guide_source_guide_reference	source_guide_reference_guide_source_guide_reference_guide_source_guide_reference	source_guide_reference_guide_source_guide_reference_guide_source_guide_reference	source_guide_reference_guide_source_guide_reference_guide_source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	This is an official DARPA program page for the Intrinsic Cognitive Security (ICS) program, which addresses vulnerabilities in mixed reality systems that could be exploited through cognitive attacks. The program aims to develop formal mathematical methods that guarantee mixed reality designs can protect users against adversarial interference.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[170, 2026]	Intrinsic Cognitive Security (ICS) - Higher-Gov	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A Higher-Gov listing for the DARPA Intrinsic Cognitive Security (ICS) research solicitation, which seeks to develop tactical mixed-reality systems that protect users against cognitive attacks using formal methods with cognitive safeguards. The program is structured as a 36-month effort in two 18-month phases, with defined funding ranges for a mixed-reality cognition technical area and an evaluation technical area.
[171, 2026]	DARPA Preps Program to Protect Mixed Reality Users	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	DARPA is putting together the Intrinsic Cognitive Security (ICS) research program “to build.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[172, 2026]	The Ethics of Cognitive Security - YorkSpace	source_guide_reference_guide_source_guide_reference_guide_source_guide_reference_guide_source_guide_reference_guide_source_guide_reference_guide_source_guide_reference_guide	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	This 2023 York University doctoral dissertation by Andrew Ward Buzzell provides an ethical and epistemic assessment of state power exercised to defend against information threats, a domain the author terms cognitive security.
[173, 2026]	Epistemic Security - Elizabeth Seger	source_guide_reference_guide_source_guide_reference_guide_source_guide_reference_guide_source_guide_reference_guide_source_guide_reference_guide_source_guide_reference_guide	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A project page from AI governance and ethics researcher Elizabeth Seger introducing the concept of epistemic security: protecting the processes through which information is created, distributed, and consumed in society. It discusses information threats to democracies such as disinformation, eroding trust in institutions, polarization, and the misuse of generative AI, and how technologies shape knowledge production.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[174, 2026]	Epistemic Security 2029: Fortifying the UK's Information Supply	source guide	reference guide	reference guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A February 2025 Demos report by Elizabeth Seger, Hannah Perry, and Jamie Hancock on strengthening the UK's information supply chain. It frames epistemic security, securing healthy and robust flows of trustworthy information, as essential to countering what it calls a democratic emergency driven by institutional distrust, the decline of local news, and concentrated control of information by social media platforms.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[175, 2026]	Tackling threats to informed decision-making in democratic societies	source_guide_reference_guide_source_guide_reference_guide_source_guide_reference_guide_

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[177, 2026]	Understanding the neurocognitive mechanisms of cognitive security	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A peer-reviewed review article published in Neuroscience & Biobehavioral Reviews (December 2025) by Crum and colleagues examining the neurocognitive mechanisms of cognitive security. The authors synthesize research on why people fall victim to false or deceptive information, proposing that certain brain systems are more exploitable than others.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[178, 2026]	Neuro-cognitive approaches to cyber-security: a systematic review	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A January 2026 systematic review in Information and Computer Security by the researcher Kritika, titled "Neuro-cognitive approaches to cyber-security." It integrates findings from neuroscience and cognitive psychology to analyze the human factor in security, examining how cognitive and neurological insights can improve security awareness education, behavioral policy development, insider threat detection, and user interface design.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[179, 2026]	Survey of Metrics for Cognitive Load in Intelligence Community	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	An NCSU Laboratory for Analytic Sciences article summarizing a systematic survey of metrics for measuring cognitive load in intelligence-analysis and similar settings. Reviewing 125 articles published between 1998 and 2024, it identifies 129 distinct metrics grouped into non-biometric methods (questionnaires such as NASA-TLX, task performance, interaction tracking) and biometric methods (eye tracking, heart rate).

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[180, 2026]	Why Psychology of Intelligence Analysis Still Matters?	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A SpecialEurasia article (2024) reviewing Richards J. Heuer Jr.'s 1999 work Psychology of Intelligence Analysis and arguing for its continued relevance. It summarizes Heuer's account of how cognitive biases such as confirmation bias, anchoring, and availability heuristics distort analytic judgment, and how analysts' backgrounds shape interpretation.
[181, 2026]	Effectiveness of training actions aimed at improving critical thinking	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Particularly noteworthy in this field is the resurgence of the cognitive inoculation theory.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[182, 2026]	Psychological Inoculation for Credibility Assessment, Sharing	source guide	reference guide	reference guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A 2023 meta-analysis in the Journal of Medical Internet Research evaluating psychological inoculation, or prebunking, as a strategy against misinformation, drawing on 42 studies with over 42,000 participants. It reports bounded improvements in people's ability to distinguish misinformation from real information, while finding limited effect on intentions to share misinformation and leaving context, durability, and transfer conditions for review.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[183, 2026]	Prebunking interventions based on “inoculation” theory can reduce	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A 2020 peer-reviewed study in the Harvard Kennedy School Misinformation Review by Roozenbeek, van der Linden, and Nygren testing the Bad News game as a prebunking intervention grounded in inoculation theory. Players take the role of a misinformation creator to learn common manipulation techniques such as impersonation, emotional appeals, polarization, and conspiratorial framing, building resistance to deceptive content.
[184, 2026]	Psychological inoculation against misinformation	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Sander van der Linden is Professor of Social Psychology in Society in the Department of Psychology.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[185, 2026]	“Inoculation” to Resist Misinformation - PubMed	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A 2024 JAMA Insights article by Sander van der Linden and Jon Roozenbeek on “inoculation” or prebunking as a psychological technique for resisting misinformation. Part of the journal’s Communicating Medicine series, it describes how preparing audiences in advance can build cognitive resistance to misleading narratives, drawing an analogy to how vaccines build immunity.
[186, 2026]	Psychological Inoculation against Misinformation: Current Evidence and Future Directions - Cecilie S. Traberg, Jon Roozenbeek, Sander van der Linden, 2022	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Much like a viral contagion, misinformation can spread rapidly from one individual to another.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[187, 2026]	INOCULATION THEORY AND MISINFORMATION	source guide reference	source guide reference	source guide reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A 2021 report published by the NATO Strategic Communications Centre of Excellence, authored by Jon Roozenbeek and Sander van der Linden of the Cambridge Social Decision-Making Lab, on inoculation theory and misinformation. It explores how psychology and behavioural science can help mitigate the spread of false and misleading information, noting that no single intervention through algorithms, legislation, or content moderation is sufficient.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[188, 2026]	From Spycraft to Self-Mastery: How Structured Analytic Techniques	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	An article on Spotter Up by Eugene Nielsen arguing that structured analytic techniques (SATs) developed for intelligence analysis can improve everyday decision-making. It describes cognitive biases such as confirmation bias and overconfidence, then outlines categories of SATs including diagnostic, contrarian, imaginative, structuring, and decision-support methods.
[189, 2026]	A Tradecraft Primer - CSI	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	This primer will assist analysts in dealing with the perennial problems of intelligence.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[190, 2026]	Objectivity - Intelligence.gov	source_guide	reference_guide	reference_guide	reference_guide	source_guide_import	source_guide_lifecycle	source_guide_context	bibliography_traceability	source_guide_context	A page on Intelligence.gov, the U.S. Intelligence Community's public site, presenting objectivity as a core IC value. It explains that intelligence analysis must be performed and conveyed without distortion from personal or political bias, and references the standards codified in Intelligence Community Directive (ICD) 203 on analytic standards.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[191, 2026]	Richards Heuer	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A Wikipedia biography of Richards J. Heuer Jr. (1927-2018), a long-serving CIA intelligence analyst known for foundational contributions to analytic tradecraft. It describes his development of the Analysis of Competing Hypotheses method, his book 'Psychology of Intelligence Analysis' arguing that structured tools help analysts cope with cognitive bias and uncertainty, and his co-authored guide to Structured Analytic Techniques.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[192, 2026]	The Psychology of Intelligence Analysis	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	Psychology of Intelligence Analysis by Richards J. Heuer Jr., published by the Center for the Study of Intelligence, Central Intelligence Agency (1999). This foundational text examines the cognitive processes and mental limitations that affect intelligence analysts, focusing on how perception, memory, and bias shape judgment. It presents structured analytic methods intended to help analysts recognize and counteract these limitations and improve the quality of their reasoning.
[193, 2026]	Structured Analytical Techniques - Organization of American States	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	Heuer provides a number of starter questions in his book.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[194, 2026]	Structured Analytic Techniques for Intelligence Analysis	source_guide_reference	reference_guide	reference_guide_source	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A copy of "Structured Analytic Techniques for Intelligence Analysis" hosted on Scribd, a roughly 310-page professional reference on analytical methodologies for intelligence work. It presents systematic frameworks that analysts can use to process information, test hypotheses, identify patterns, and reach evidence-based conclusions while reducing bias. The document is oriented toward practitioners seeking to strengthen analytic rigor.
[195, 2026]	Full article: Analytic Tradecraft and the Intelligence Community	source_guide_reference	reference_guide	reference_guide_source	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The emphasis and visibility afforded analytic tradecraft in the Intelligence Community's analytic.
[196, 2026]	Analytic Tradecraft Standards - Army University Press	source_guide_reference	reference_guide	reference_guide_source	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The nine analytic tradecraft standards in Intelligence Community Directive (ICD) 203, Analytic.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[197, 2026]	Getting Things Done: The Science behind Stress-Free Productivity	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	In 2001 David Allen proposed 'Getting Things Done' (GTD) as a method for enhancing personal.
[198, 2026]	Metoda GTD = Getting Things Done - Lukáš Barda	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A Czech-language explainer of the Getting Things Done (GTD) productivity method created by David Allen. It describes the system's core steps of capturing thoughts, clarifying them into actionable items, organizing and prioritizing, regularly reviewing, and executing, including the principle of doing any task that takes under two minutes immediately. The page also surveys software tools for implementing GTD, such as Todoist, OmniFocus, Trello, Evernote, and Notion.
[199, 2026]	David Allen Explains Why GTD Improves Team Performance	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Source-guide bibliography entry.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[200, 2026]	The Science Behind Flow State / Achieving Optimal Performance	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	A marketing blog post on the Dingbats Notebooks e-commerce site about flow state and how writing tools can support it. It summarizes Mihaly Csikszentmihalyi's concept of flow as a state of full absorption marked by intense focus, clear goals, and immediate feedback, and reviews associated benefits and neuroscience such as reduced prefrontal-cortex activity and increased dopamine.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[201, 2026]	Go with the flow: A neuroscientific view on being fully engaged	source_guide_reference_guide_import	source_guide_reference_guide_lifecycle	source_guide_reference_guide_context	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A 2020 theoretical review article in the European Journal of Neuroscience by van der Linden, Tops, and Bakker proposing a neuroscientific model of flow, the state of full task absorption with strong drive and low self-referential thinking. The authors argue that the dopamine and norepinephrine systems drive the motivational and mood components of flow, and that interaction among the default mode, central executive, and salience networks produces its characteristic features.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[202, 2026]	Flow (psychology)	source guide	reference guide	reference guide	reference guide	source guide lifecycle	source guide context	bibliography traceability	source guide context	A Wikipedia article on flow, the psychological state of complete immersion and focused engagement in an activity, also known as being in the zone. It traces the concept to psychologist Mihaly Csikszentmihalyi and describes flow as a balance between challenge and skill, characterized by intense concentration, merging of action and awareness, loss of self-consciousness, a sense of control, distorted time perception, and intrinsic reward.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[203, 2026]	How Flow Theory Unleashes High Performance in Your Career	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	A blog article applying Mihaly Csikszentmihalyi's Flow Theory to workplace and career performance. It describes flow as a state of full absorption in an activity, lists conditions associated with it such as clear goals, immediate feedback, and a balance between challenge and skill, and discusses how time can appear distorted during flow. The piece argues that achieving flow states enhances productivity and job satisfaction across roles and industries.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[204, 2026]	The Neuroscience of Flow State: How the Brain Reaches Peak	source_guide_reference_guide_source_guide_reference_guide_source_guide_reference_guide_

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[205, 2026]	Flow Research Collective: Neuroscience of Human Performance	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	This is the website of the Flow Research Collective, a research and development organization founded in 2018 that studies the neuroscience of human performance and brain health. It investigates flow states of focused absorption and applies that research to peak performance training for organizations as well as to mental health conditions such as PTSD and depression.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[206, 2026]	Investigating the “Flow” Experience: Key Conceptual	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	A 2020 conceptual analysis by Sami Abuhamdeh in Frontiers in Psychology arguing that flow research has stalled because the construct is operationalized inconsistently across studies. It identifies disagreements over whether flow is a discrete state or a continuum, whether enjoyment is essential to it, and whether scales conflate flow’s conditions with the experience itself.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[207, 2026]	The Cognitive Load – Productivity Tradeoff in Task Switching	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A 2023 research article in the Proceedings of the Human Factors and Ergonomics Society Annual Meeting by Maximillian Chis and colleagues examining task switching during team-based search-and-rescue scenarios in Minecraft. Using an ACT-R model of working memory, the study found that teams switching between task sets less frequently showed both higher cognitive load and higher performance scores.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[208, 2026]	Securing Industrial Control Systems: Components, Cyber Threats	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	This article provides a comprehensive overview of cybersecurity for Industrial Control Systems, covering SCADA, distributed control systems, and programmable logic controllers as they have evolved from isolated architectures to networked, cloud-connected deployments.
[209, 2026]	What are Industrial Control Systems (ICS)? / Bitsight	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A glossary entry from the cybersecurity company Bitsight explaining Industrial Control Systems (ICS), defined as integrated hardware and software used to control, monitor, and automate industrial processes across manufacturing, energy, and critical infrastructure.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[210, 2026]	What Are the Differences Between OT, ICS, & SCADA Security?	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A Palo Alto Networks Cyberpedia article explaining the relationship among operational technology (OT), industrial control system (ICS), and SCADA security.
[211, 2026]	The 2026 Cybersecurity Guide to Industrial Control Systems - Claroty	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A Claroty guide to securing industrial control systems (ICS) amid IT and operational technology convergence. It identifies challenges including an expanded attack surface, legacy systems lacking modern protections, third-party access gaps, patching delays due to uptime requirements, and advanced adversaries targeting ICS.
[212, 2026]	Operational Technology Cybersecurity - Idaho National Laboratory	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Source-guide bibliography entry.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[213, 2026]	ICS Matrix - MITRE ATT&CK®	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	The Industrial Control Systems (ICS) domain of the MITRE ATT&CK framework, a knowledge base documenting adversary behaviors based on real-world observations of attacks on critical infrastructure. The matrix organizes methods into twelve tactical categories spanning initial access through impact, including ICS-specific concerns such as firmware modification and disruption of operational technology.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[214, 2026]	Cybersecurity Using ICS ATT&CK Strategies	source guide reference	source guide reference	source guide reference	source guide reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	A June 2021 InTech Magazine article by Jacob Chapman, published by the International Society of Automation, on using the ICS ATT&CK framework to strengthen cybersecurity for manufacturing and industrial IoT systems. It describes a three-phase risk-management approach: gathering information on assets and network architecture, mapping potential attack paths to identify vulnerabilities, and prioritizing mitigations by impact.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[215, 2026]	MITRE ATT&CK for ICS Framework - Dragos	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	A Dragos solutions page describing the MITRE ATT&CK for ICS framework, a knowledge base of adversary behaviors observed in attacks against industrial control system networks. It explains how the Dragos Platform maps detections to ATT&CK tactics and techniques through regular knowledge updates, profiles named threat groups, and organizes behaviors across tactic areas spanning initial access through impact scenarios such as loss of control, safety, or availability.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[216, 2026]	How to Use the MITRE ATT&CK Framework for ICS - Nozomi Networks	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A Nozomi Networks resource (a 2020 webinar) on how security teams apply the MITRE ATT&CK framework for Industrial Control Systems. It explains that the ICS version is a community-sourced knowledge base mapping adversary tactics and behaviors specific to industrial environments, distinct from the IT-focused framework.
[217, 2026]	An evaluation framework for industrial control system cyber incidents	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	We analyze six significant ICS cyber incidents in the energy and power industries, namely Stuxnet.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[218, 2026]	THE CYBER-PHYSICAL SIX / Honeywell	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	An executive research report from Honeywell's Global Analysis, Research, and Defense group titled "The Cyber-Physical Six," tracing how targeted industrial attacks have evolved and predicting future trends. It reviews six landmark cyber-physical attacks affecting industrial control and operational technology systems, then analyzes observed trends such as modularity, expanding capabilities, and the increasing frequency of new attack tools.
[219, 2026]	Stuxnet 15 Years Later and the Evolution of Cyber Threats to Critical	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	I've been asked specifically to describe how.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[220, 2026]	Zetter details how Stuxnet marked a turning point in cyberwarfare	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Journalist Kim Zetter testified before Congress on how Stuxnet demonstrated that physical infrastructure could be destroyed through malicious code alone, targeting Siemens programmable logic controllers at Iran's Natanz uranium enrichment facility.
[221, 2026]	About	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Presidential Policy Directive 28 (PPD-28), Signals Intelligence Activities, in the ODNI IC Legal Reference Book, establishing principles and safeguards (data minimization and protections for personal information regardless of nationality) that govern U.S. signals intelligence collection and use.
[222, 2026]	CIA - National Archives	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The scope of the CIA mission is vast and the complexities of intelligence tradecraft.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[223, 2026]	Active-Measures-and-Information-Wars - Central Intelligence Agency	source_guide_reference_guide_source_guide_reference	source_guide_reference_guide_source_guide_reference	source_guide_reference_guide_source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A book review article by J. E. Leonardson (a CIA Directorate of Analysis analyst writing under a pen name), published in Studies in Intelligence Vol. 64, No. 1 (March 2020).
[224, 2026]	Cyber Kill Chain® / Lockheed Martin	source_guide_reference_guide_source_guide_reference	source_guide_reference_guide_source_guide_reference	source_guide_reference_guide_source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A Lockheed Martin capabilities page describing the Cyber Kill Chain, a framework that is part of the company's Intelligence Driven Defense model for identifying and preventing cyber intrusions. It frames intrusions as a sequence of stages an adversary must complete to achieve an objective, with the aim of improving defenders' visibility into attacker behavior, and is oriented toward defending against advanced persistent threats.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[225, 2026]	AI Agents vs. Agentic AI: A Conceptual taxonomy, applications	source_guide	reference_guide	reference_guide	reference_guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Illustration of the three core characteristics defining AI Agents: autonomy, task-specificity.
[226, 2026]	Agentic AI: A Comprehensive Survey of Technologies, Applications	source_guide	reference_guide	reference_guide	reference_guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A robust multidimensional taxonomy is proposed that classifies agents based on their structural.
[227, 2026]	AI Agent Frameworks: Choosing the Right Foundation for Your … - IBM	source_guide	reference_guide	reference_guide	reference_guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	An IBM Think Insights article comparing leading AI agent frameworks to help teams choose a foundation for building agentic systems. It surveys open-source orchestration frameworks for single- and multi-agent solutions, including CrewAI and AutoGen, and discusses considerations such as workflow orchestration, collaboration among agents, and integration. The article is written as a practitioner-oriented overview of the framework landscape.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[228, 2026]	AGI-Edgerunners/LLM-Agents-Papers	source_guide_reference_guide_source_guide_reference_guide_source_guide_reference_guide_source_guide_reference_guide_source_guide_reference_guide_source_guide_reference_guide			source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A curated GitHub repository (AGI-Edgerunners/LLM-Agents-Papers) collecting research papers on large language model based agents, last updated July 2025. It organizes work into categories including survey papers, enhancement techniques such as planning, memory, feedback, retrieval, and search, agent interactions like tool usage and conversation, domain applications, training methods, multi-agent systems, safety, and benchmarks.
[229, 2026]	How Different Types of AI Agents Work - [x]cube LABS	source_guide_reference_guide_source_guide_reference_guide_source_guide_reference_guide_source_guide_reference_guide_source_guide_reference_guide_source_guide_reference_guide			source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	It explores the taxonomy of agents, bridging the gap between classical artificial intelligence.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[230, 2026]	Karl Friston Explains Active Inference & AI Break-throughs - YouTube	source_guide_reference_guide_source_guide_reference_guide_source_guide_reference_guide_

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[231, 2026]	The Secret History of Disinformation and Political Warfare - CSI	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	The CIA Studies in Intelligence URL for 'The Secret History of Disinformation' returns 404. The article by Thomas Rid on political warfare history is accessible through the CIA CSI portal at an updated path; verify the URL before citation.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[232, 2026]	European AI Office	source guide reference	source guide reference	source guide reference	source guide reference import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The European AI Office is the European Commission's central hub for developing and implementing AI governance across the EU, established to support trustworthy AI adoption while protecting people from associated risks. Its responsibilities include enforcing regulations for general-purpose AI models, implementing the AI Act, developing evaluation tools and benchmarks for assessing AI capabilities, and investigating potential regulatory violations.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[233, 2026]	General-Purpose AI Code of Practice	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	An official European Commission Digital Strategy webpage documenting the General-Purpose AI Code of Practice, a voluntary guidance document helping general-purpose AI providers comply with the EU AI Act's rules on safety, transparency, and copyright. It describes an iterative drafting process involving nearly 1,000 stakeholders across four working groups, running from September 2024 through July 2025.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[234, 2026]	AI Act	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	The European Commission's official page on the AI Act, described as the first comprehensive legal framework on artificial intelligence worldwide. It explains the regulation's risk-based approach, classifying AI systems into unacceptable, high, transparency, and minimal risk tiers, with prohibited practices and strict requirements for high-risk uses.
[235, 2026]	ISO/IEC 42005:2025 AI System Impact Assessment	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	ISO standard page for AI system impact assessment.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[236, 2026]	ISO/IEC TR 24028:2020 Artificial Intelligence Trustworthiness Overview	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	The ISO catalog page for ISO/IEC TR 24028:2020, a technical report titled "Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence." The document surveys topics related to AI trustworthiness, including approaches to establishing trust through transparency, explainability, and controllability, and approaches to assess and achieve availability, resilience, reliability, accuracy, safety, security, and privacy of AI systems.
[237, 2026]	Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	Official GAO AI accountability framework.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[238, 2026]	Recommendation on the Ethics of Artificial Intelligence	source guide reference	source guide reference	source guide reference	source guide reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	The official UNESCO page for the Recommendation on the Ethics of Artificial Intelligence, the first global standard-setting instrument on AI ethics, adopted in 2021 and applicable to all 194 member states. It outlines four core values, including human rights protection and environmental flourishing, and ten guiding principles such as proportionality, privacy, transparency, and fairness.
[239, 2026]	Digital Space and Human Rights	source guide reference	source guide reference	source guide reference	source guide reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	Official OHCHR digital rights portal.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[240, 2026]	The Right to Privacy in the Digital Age	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The Office of the High Commissioner for Human Rights (OHCHR) hub page on the right to privacy in the digital age. It addresses how data-intensive technologies, particularly artificial intelligence, create risks for privacy, autonomy, and human dignity, and curates international standards, reports, and expert consultations.
[241, 2026]	Modernised Convention 108	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Official Council of Europe Convention 108+ source.
[242, 2026]	Guidance for Generative AI in Education and Research	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Official UNESCO generative AI education guidance.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[243, 2026]	AI Competency Frameworks for Teachers and Students	source_guide_reference	guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	A UNESCO announcement of two new AI competency frameworks, one for students and one for teachers, intended to guide safe and responsible engagement with artificial intelligence in education. The student framework emphasizes a human-centered perspective, ethical use, foundational AI knowledge, and design thinking, while the teacher framework covers ethics, technical understanding, and pedagogy.
[244, 2026]	AI and Education	source_guide_reference	guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	Official UNESCO GEM AI and education source hub.
[245, 2026]	Artificial Intelligence in Education	source_guide_reference	guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	Official OECD AI in education topic page.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[246, 2026]	Digital Education Action Plan 2021-2027	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	The European Commission's official page on the Digital Education Action Plan (2021-2027), a strategic framework for promoting high-quality, inclusive digital learning across EU education systems. It defines digital education as the use of digital tools, technologies, and content to support teaching, learning, and assessment, and cites pandemic-driven adoption alongside persistent gaps in teacher readiness, student digital skills, and household access.
[247, 2026]	AI in the Public Sector	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	Official OECD.AI public-sector AI theme page.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[248, 2026]	Artificial Intelligence Working Group	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The World Bank GovTech program page for its Artificial Intelligence Working Group, a community of government technology experts focused on knowledge-sharing and policy tools for responsible public-sector AI adoption. It notes that many developing countries face barriers such as limited digital skills, infrastructure, and data, which risk widening global inequality.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[249, 2026]	GgovTech: Putting People First	source_guide	reference_guide	reference_guide	reference_guide	source guide lifecycle	source guide context	bibliography traceability	source guide context	The official page for the World Bank's Global Program on GovTech and Public Sector Innovation, which helps governments use technology and data to improve public services and governance. It describes support for digital transformation in public administration across areas such as tax administration, public financial management, human resource systems, and citizen engagement, with cross-cutting themes including responsible AI and green digital transformation.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[250, 2026]	AI Guide for Government	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The official U.S. government AI.gov website presenting the federal administration's artificial intelligence strategy. It is organized around an AI Action Plan built on three pillars: accelerating innovation, building infrastructure, and leading international AI diplomacy. The site compiles executive orders, policy documents and OMB memos on government AI adoption, education initiatives, and leadership remarks, framing AI development as central to U.S. global competitiveness.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[251, 2026]	European Data Governance Act	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The European Commission page explaining the Data Governance Act, an EU regulation that became applicable in September 2023 to build trust in data sharing and ease reuse of data. It outlines four mechanisms: facilitating reuse of protected public-sector data, establishing trusted data intermediaries, enabling voluntary data sharing by citizens and businesses, and removing barriers to cross-sector and cross-border data use.
[252, 2026]	Data Act Explained	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	An official European Commission explainer on the EU Data Act, which became applicable on 12 September 2025.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[253, 2026]	Common European Data Spaces	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	This is an official European Commission webpage describing the Common European Data Spaces initiative, part of the EU strategy to create interconnected, trustworthy data-sharing environments across strategic sectors. It explains that data spaces let organizations and individuals share data while retaining control, guided by principles of open participation, privacy protection, and fair access rules.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[254, 2026]	A European Strategy for Data	source_guide_reference_guide_reference_guide_reference_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	An official European Commission page outlining the European Strategy for Data, which aims to create a single market for data to support competitiveness and data sovereignty. It describes initiatives such as Common European Data Spaces, opening high-value public datasets, and investment in cloud and data-processing capacity, supported by the Data Governance Act and the Data Act. The page frames data sharing as a driver of innovation balanced with privacy and European values.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[255, 2026]	Web of Things (WoT) Architecture 1.1	source_guide	reference_guide	reference_guide	reference_guide	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The W3C Recommendation for Web of Things Architecture 1.1, published in December 2023, defining an abstract architecture for interoperability across diverse Internet of Things platforms. It introduces core concepts including Things described by machine-readable Thing Descriptions, reusable Thing Models, and Consumers that interpret descriptions to interact via Properties, Actions, and Events.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[256, 2026]	Web of Things (WoT) Thing Description 1.1	source_guide	reference_guide	reference_guide	reference_guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The W3C WoT Thing Description 1.1 is a formal information model and standardized representation format enabling IoT devices to describe their metadata and interaction capabilities in a machine-readable way, facilitating interoperability across diverse ecosystems.
[257, 2026]	Web of Things (WoT) Discovery	source_guide	reference_guide	reference_guide	reference_guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A W3C Recommendation for Web of Things (WoT) Discovery, published December 5, 2023 by the W3C Web of Things Working Group. It specifies how IoT devices and services can be discovered and how their Thing Description metadata can be accessed securely, using a two-phase model of Introduction and Exploration.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[258, 2026]	OpenAPI Specification	source guide reference	reference guide	reference guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The official OpenAPI Initiative publications page, serving as a central index for the OpenAPI Specification and related standards including the Arazzo and Overlay specifications. It provides access to multiple specification versions (2.0, 3.0, 3.1, and 3.2) and their corresponding downloadable schemas identified by release date, along with a registry of extensions, formats, media types, and other resources.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[259, 2026]	Verifiable Credentials Data Model v2.0	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The W3C Verifiable Credentials Data Model v2.0 Recommendation, which specifies how to express digital credentials on the web in a cryptographically secure, privacy-respecting way. It defines an extensible data model for tamper-evident assertions made by an issuer about a subject, within a three-party ecosystem of issuers, holders, and verifiers supported by verifiable data registries.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[260, 2026]	Decentralized Identifiers (DIDs) v1.0	source_guide	reference_guide	reference_guide	reference_guide	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The W3C Recommendation for Decentralized Identifiers (DIDs) v1.0, published July 2022, defining a type of identifier that enables verifiable digital identity without reliance on a centralized registration authority. It specifies DID syntax (a scheme, method name, and method-specific identifier) and the DID document data model, which expresses verification methods, services, controllers, and verification relationships for authentication and assertion.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[261, 2026]	RFC 9110: HTTP Semantics	source_guide_reference_guide	reference_guide	reference_guide	reference_guide	source guide lifecycle	source guide context	bibliography traceability	source guide context	RFC 9110, the official IETF standards document defining the core semantics and architecture of HTTP, published in June 2022 and consolidating nine earlier RFCs. It establishes terminology and protocol aspects shared across HTTP versions, including methods, status codes, header fields, content negotiation, conditional and range requests, authentication, and the http and https URI schemes.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[262, 2026]	Artificial Intelligence	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	The International Labour Organization's topic portal on artificial intelligence and the world of work. It examines AI's dual role in automating worker tasks and in automating managerial functions through algorithmic management, arguing that whether AI displaces or complements jobs depends on how technology is integrated into work processes.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[263, 2026]	Mind the AI Divide: Shaping a Global Perspective on the Future of Work	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A joint UN and International Labour Organization report (July 2024) titled 'Mind the AI Divide,' examining how unequal AI adoption can deepen global inequality. It argues that disparities in digital infrastructure, technology, education, and training risk leaving less developed nations further behind as economies shift toward AI-driven production.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[264, 2026]	Global Commission on the Future of Work	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	An International Labour Organization news article (January 2019) announcing the findings of the ILO Global Commission on the Future of Work, a 15-month study co-chaired by the leaders of South Africa and Sweden. The commission issued ten recommendations addressing workplace change driven by technological and demographic shifts, including universal labor protections, lifelong learning, and stronger social safety nets.
[265, 2026]	AI and Work	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Official OECD.AI work theme page.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[266, 2026]	PROV Overview	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A W3C Working Group Note from 2013 that provides an overview and roadmap for the PROV family of specifications for representing and exchanging provenance information on the web. It defines provenance as information about the entities, activities, and people involved in producing data, used to assess quality, reliability, and trustworthiness.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[267, 2026]	PROV-O: The PROV Ontology	source_guide_reference_guide_reference_guide_reference

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[268, 2026]	Data Catalog Vocabulary (DCAT) Version 3	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	DCAT Version 3 is a W3C RDF vocabulary designed to facilitate interoperability between data catalogs published on the web, enabling organizations to describe datasets and data services using standardized terminology for improved discoverability and federated search. The specification organizes catalog metadata around seven core classes including Catalog, Dataset, Distribution, Data Service, and Dataset Series, drawing on established vocabularies such as Dublin Core and FOAF.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[269, 2026]	Data on the Web Best Practices	source_guide	reference_guide	reference_guide	reference_guide	source_guide reference_guide import	source_guide lifecycle	source_guide context	bibliography traceability	source_guide context	A W3C Recommendation, “Data on the Web Best Practices,” published January 31, 2017 by the Data on the Web Best Practices Working Group. It offers 35 best practices for publishing and consuming data on the Web, covering metadata, licensing and provenance, data quality, dataset versioning, persistent URIs, machine-readable formats, vocabulary reuse, access methods, preservation, and feedback.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[270, 2026]	NIST Big Data Interoperability Framework	source_guide	reference_guide	reference_guide	reference_guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	NIST Special Publication 1500-1 (revised edition by Chang and Grady) establishes foundational terminology and consensus definitions for Big Data through the NIST Big Data Public Working Group. The volume defines Big Data characteristics, taxonomy, and a reference architecture assigning roles to Application Providers, Data Consumers, Data Providers, and System Orchestrators.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[271, 2026]	DataCite Metadata Schema	source_guide	reference_guide	reference_guide	reference_guide	source guide lifecycle	source guide context	bibliography traceability	source guide context	The DataCite Metadata Schema page, introducing a standardized framework of core metadata properties chosen for accurate and consistent identification of research resources for citation and retrieval. It notes the latest version, 4.7 (March 2026), which adds resource types such as Poster and Presentation along with new identifier and relation-type options.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[272, 2026]	C2PA Specifications	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	The specifications hub for the C2PA (Coalition for Content Provenance and Authenticity), a standards initiative that develops technical methods for certifying the source and history of media content to counter misleading information. It publishes the core Content Credentials specification along with related material such as attestations and a soft-binding API, plus implementation, security, and user-experience guidance including for AI-generated content.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[273, 2026]	WCAG 2 Overview	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The W3C Web Accessibility Initiative overview of the Web Content Accessibility Guidelines (WCAG), an international standard for making web content accessible to people with disabilities. It explains that WCAG is organized around four principles (perceivable, operable, understandable, robust) with testable success criteria at three conformance levels (A, AA, AAA), and covers versions 2.0, 2.1, and 2.2.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[274, 2026]	CAST Universal Design for Learning Guidelines version 3.0	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The official CAST website for the Universal Design for Learning (UDL) Guidelines version 3.0, released in 2024. The framework offers research-based guidance for designing inclusive learning environments and is organized around three principles: Engagement (motivation and emotional support), Representation (accessible presentation of information), and Action and Expression (diverse means of participation and communication).

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[275, 2026]	Fact Sheet: New Rule on the Accessibility of Web Content and Mobile Apps Provided by State and Local Governments	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	A US Department of Justice fact sheet explaining the 2024 ADA Title II rule requiring state and local governments to make their web content and mobile apps accessible. It establishes WCAG 2.1 Level AA as the technical standard, applies to entities such as schools, courts, libraries, and transit agencies, and sets compliance deadlines of April 2027 for larger jurisdictions and April 2028 for smaller ones.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[276, 2026]	What is a Data Protection Impact Assessment and When Is This Mandatory?	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A European Data Protection Board FAQ page, part of its data protection guide for small businesses, explaining Data Protection Impact Assessments (DPIAs) and when they are mandatory. It describes a DPIA as a written assessment of the impact of a planned processing operation, required when processing poses high risks to individuals' rights.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[277, 2026]	Endorsed WP29 Guidelines	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	This is a European Data Protection Board webpage listing guidelines and documents originating from the Article 29 Working Party that the EDPB endorsed at its first plenary meeting. The catalogued materials relate to the GDPR and cover topics such as consent and transparency, data breach notification, automated decision-making and profiling, data protection impact assessments, data protection officers, and binding corporate rules.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[278, 2026]	Recommendation of the Council on Public Procurement	source guide	reference guide	reference guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The OECD Recommendation of the Council on Public Procurement (OECD/LEGAL/041 a legal instrument adopted by the OECD Council in 2015 on the proposal of the Public Governance Committee. It frames public procurement as a pillar of strategic governance and service delivery and sets out principles for governments to follow.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[279, 2026]	Open Contracting Data Standard	source_guide	reference_guide	reference_guide	reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The documentation homepage for the Open Contracting Data Standard, version 1.1.5, maintained by the Open Contracting Partnership to support disclosure of government contracting data across the procurement lifecycle. It provides a common data model spanning planning, tender, award, contract, and implementation stages, along with a primer, implementation guidance, technical schemas, and validation tooling.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[280, 2026]	NIST SP 800-61 Rev. 3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	NIST SP 800-61 Rev. 3, published April 2025, integrates incident response guidance into broader cybersecurity risk management aligned with the NIST Cybersecurity Framework 2.0, superseding the 2012 Rev. 2. The publication addresses cyber threat information sharing, incident handling and management practices, and procedures for detecting, responding to, and recovering from security incidents.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[281, 2026]	Artificial Intelligence Cybersecurity Challenges	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	An ENISA (European Union Agency for Cybersecurity) report published December 15, 2020 mapping the cybersecurity challenges of artificial intelligence. It defines AI scope through a lifecycle approach, identifies the assets requiring protection within AI ecosystems, and develops a threat taxonomy classified across lifecycle stages and asset categories.
[282, 2026]	AI Research: Security and Resilience	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	A NIST page on AI research focused on security and resilience, framing these as core characteristics of trustworthy AI under the NIST AI Risk Management Framework.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[283, 2026]	Recommendation of the Council on Open Government	source guide	reference guide	reference guide	reference guide	source guide lifecycle	source guide context	bibliography traceability	source guide context	An OECD legal instrument document reproducing the Recommendation of the Council on Open Government (OECD/LEGAL/043 adopted on 14 December 2017. It defines open government as a culture of governance promoting transparency, integrity, accountability, and stakeholder participation in support of democracy and inclusive growth.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[284, 2026]	Verifiable Credential Data Integrity 1.0	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The W3C Recommendation for Verifiable Credential Data Integrity 1.0, published May 2025, defining mechanisms for ensuring the authenticity and integrity of verifiable credentials using cryptographic proofs. It specifies a process of data transformation, hashing, and proof generation, and a corresponding verification procedure, along with a proof data model containing properties such as type, verification method, purpose, and proof value.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[285, 2026]	NIST AI Resource Center	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The NIST AI Resource Center (AIRC), a government platform supporting implementation of the NIST AI Risk Management Framework, a voluntary framework for managing AI risk. It provides the core framework along with a playbook of practical actions, profiles tailored to specific sectors and technologies, use cases, and crosswalks linking the framework to other governance structures.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[286, 2026]	Model Cards for Model Reporting	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The arXiv abstract for “Model Cards for Model Reporting” (2018) by Mitchell, Wu, Zaldivar, and colleagues, which introduces a framework for transparent documentation of machine learning models. Model cards are short accompanying documents that report a model’s benchmarked performance across varied conditions, including different cultural, demographic, and phenotypic groups, along with intended use, evaluation methodology, and deployment considerations.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[287, 2026]	Datasheets for Datasets	source guide reference	source guide reference	source guide reference	source guide reference import	source guide lifecycle	source guide context	bibliography traceability	source guide context	A 2018 arXiv paper proposing ‘datasheets for datasets,’ a standardized documentation framework for machine learning datasets modeled on electronic component datasheets. The authors argue the field lacks consistent dataset documentation, which creates risk in high-stakes applications, and propose that datasets be accompanied by documentation covering motivation, composition, collection process, recommended uses, and test results.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[288, 2026]	Algorithmic Transparency Recording Standard Hub	source_guide	reference_guide	reference_guide	reference_guide	source guide lifecycle	source guide context	bibliography traceability	source guide context	A GOV.UK collection page serving as the hub for the UK Algorithmic Transparency Recording Standard (ATRS), maintained by the Government Digital Service. It provides a standardized template for documenting public-sector use of algorithmic tools, completion guidance, policy on scope and compliance, and a searchable repository of published transparency records.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[289, 2026]	Guidance for Organisations Using the Algorithmic Transparency Recording Standard	source_guide_reference	reference_guide	reference_guide	reference_guide_import	source_guide_lifecycle	source_guide_context	bibliography_traceability	source_guide_context	This is a GOV.UK guidance page published by the Government Digital Service that instructs public sector organizations on completing the Algorithmic Transparency Recording Standard (ATRS) template and publishing their records to the GOV.UK repository. It applies both to central government bodies required to publish under mandatory policy and to other public sector bodies doing so voluntarily.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[290, 2026]	NIST SP 800-218A: Secure Software Development Practices for Generative AI and Dual-Use Foundation Models	source_guide_reference	reference_guide	reference_guide	reference_guide_import	source_guide_lifecycle	source_guide_context	bibliography_traceability	source_guide_context	NIST Special Publication 800-218A (July 2024), which augments the Secure Software Development Framework with practices specific to AI model development across the software lifecycle. Produced in response to Executive Order 14110, it addresses AI model producers, developers building on those models, and acquirers of AI systems, and is designed to be used alongside NIST SP 800-218.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[291, 2026]	Revised 508 Standards and 255 Guidelines	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Official documentation from the U.S. Access Board on the Revised 508 Standards and 255 Guidelines for information and communication technology accessibility. It establishes mandatory accessibility requirements for federal agencies and voluntary guidelines for telecommunications manufacturers, covering hardware, software, websites, electronic documents, and support services.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[292, 2026]	Assessing Risks and Impacts of AI (ARIA): Pilot Evaluation Report	source guide reference	source guide reference	source guide reference	source guide reference import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The ARIA 0.1 pilot evaluation report documents NIST's methodology for systematically assessing AI applications for risks and societal impacts, using a multi-layered evaluation approach across five participating organizations and seven submitted AI applications. The pilot employed three evaluation scenarios and three testing levels: model testing, red teaming, and field testing, supplemented by dialogue annotation, tester questionnaires, and structured measurement trees.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[293, 2026]	Inventory of NARA Artificial Intelligence (AI) Use Cases	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	The National Archives and Records Administration (NARA) official inventory of its artificial intelligence use cases, documenting 14 projects across deployed, pilot, and planned stages. Deployed efforts include workplace productivity tools, automated tagging for museum experiences, and historical record retrieval, while pilots cover PII detection and redaction, semantic search, and metadata generation, and planned work targets FOIA processing and public search.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[294, 2026]	M-25-21: Accelerating Federal Use of AI through Innovation, Governance, and Public Trust	source_guide	reference_guide	reference_guide	reference_guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	An April 2025 Office of Management and Budget memorandum (M-25-21) directing executive branch agencies on federal use of artificial intelligence. Issued under Executive Order 14179, it instructs agencies to accelerate adoption of AI to improve public services and government efficiency while maintaining safeguards for civil rights, civil liberties, and privacy.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[295, 2026]	M-25-22: Driving Efficient Acquisition of Artificial Intelligence in Government	source_guide_reference	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	OMB Memorandum M-25-22 (April 3, 2025), Driving Efficient Acquisition of Artificial Intelligence in Government, issued under Executive Order 13960 and related directives. It provides guidance to federal agencies for acquiring effective and trustworthy AI in a timely, cost-effective manner, and rescinds and replaces earlier memorandum M-24-18.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[296, 2026]	Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile	source_guide_reference	reference_guide	reference_guide	reference_guide_import	source_guide_lifecycle	source_guide_context	bibliography_traceability	source_guide_context	NIST AI 600-1, the Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, a cross-sectoral companion resource to the NIST AI RMF 1.0 issued pursuant to Executive Order 14110. It identifies risks that are unique to or amplified by generative AI and organizes suggested actions for managing those risks, mapped to the AI RMF functions.
[297, 2026]	Intelligence Community Directive 203: Analytic Standards	source_guide_reference	reference_guide	reference_guide	reference_guide_import	source_guide_lifecycle	source_guide_context	bibliography_traceability	source_guide_context	Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[298, 2026]	Intelligence Community Directives	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations.
[299, 2026]	Model Context Protocol Specification	source_guide_reference	source_guide_reference	source_guide_reference	source guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation).

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[300, 2026]	MITRE ATLAS	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference import	source guide lifecycle	source guide context	bibliography traceability	source guide context	MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy.
[301, 2026]	The IC OSINT Strategy 2024-2026	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference import	source guide lifecycle	source guide context	bibliography traceability	source guide context	Official Intelligence Community strategy for open-source intelligence governance, integration, source discovery, data, tools, tradecraft, and workforce priorities.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[302, 2026]	National Geospatial-Intelligence Agency About Us	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	The official "About Us" page of the National Geospatial-Intelligence Agency (NGA), a U.S. Department of Defense and intelligence community organization. It describes NGA's mission of delivering geospatial intelligence, or GEOINT, to support military operations, policymakers, and first responders, spanning imagery analysis, mapping, geodesy, and navigation safety.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[303, 2026]	Software Security in Supply Chains	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference import	source guide lifecycle	source guide context	bibliography traceability	source guide context	An official NIST page on software supply chain security issued under Executive Order 14028, focused on the Software Bill of Materials as a formal record of software components and their supply chain. It explains the benefits of SBOMs for vulnerability identification and supply-chain transparency, recommends machine-readable formats such as SPDX, CycloneDX, and SWID, and describes foundational, sustaining, and enhancing levels of implementation.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[304, 2026]	Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences.
[305, 2026]	DevSecOps	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support.
[306, 2026]	Artificial Intelligence	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[307, 2026]	ICS Recommended Practices	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	Official CISA Industrial Control Systems recommended practices page for defensive ICS/OT safety, resilience, and incident-preparation guidance.
[308, 2026]	Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure	source_guide_reference	source_guide_reference	source_guide_reference	source_guide_reference	source guide lifecycle	source guide context	bibliography traceability	source guide context	An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[309, 2026]	STIX Version 2.1	source_guide	reference_guide	reference_guide	reference_guide	source_guide_import	source_guide_lifecycle	source_guide_context	bibliography_traceability	source_guide_context	An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[310, 2026]	TAXII Version 2.1	source_guide	reference_guide	reference_guide	reference guide import	source guide lifecycle	source guide context	bibliography traceability	source guide context	The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe).

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[311, 2026]	Countering Information Threats	source_guide	reference_guide	reference_guide	2026-05-21	source guide lifecycle	source guide context	bibliography traceability	source guide context	An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering.
[312, 2026]	Guide on the Use of Agentic Artificial Intelligence	source_guide	reference_guide	reference_guide	2026-05-21	source guide lifecycle	source guide context	bibliography traceability	source guide context	Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support.
[OECD, 2026a]	The Agentic AI Landscape and Its Conceptual Foundations	source_quality	source_quality	source_quality	2026-05-21	semiannual	curriculum maintainer, instructor, reviewer, and learner	source-quality triangulation and claim-boundary review	source transparency, accountability, and evidence traceability	Official OECD conceptual foundation for agentic AI.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of Standards and Technology, 2023]	Artificial Intelligence Risk Management Framework (AI RMF 1.0)	source_quality	source_anchor	quality_spine	2026-05-21	semiannual	curriculum maintainer, instructor, reviewer, and learner	source-quality triangulation and claim-boundary review	source transparency, accountability, and evidence traceability	Official NIST.AI.100-1 risk-management framework.
[of Standards and Technology, 2024d]	Artificial Intelligence Risk Management Framework: Generative AI Profile	source_quality	source_anchor	quality_spine	2026-05-21	semiannual	curriculum maintainer, instructor, reviewer, and learner	source-quality triangulation and claim-boundary review	source transparency, accountability, and evidence traceability	Official NIST AI 600-1 generative AI profile.
[Agency, 2025]	Security Design Considerations for AI-Driven Automation Leveraging MCP	source_quality	source_anchor	quality_spine	2026-05-21	semiannual	curriculum maintainer, instructor, reviewer, and learner	source-quality triangulation and claim-boundary review	source transparency, accountability, and evidence traceability	Official NSA security guidance for Model Context Protocol automation.
[of Standards and Technology, 2024b]	Guide to Operational Technology Security, NIST SP 800-82 Rev. 3	source_quality	source_anchor	quality_spine	2026-05-21	semiannual	curriculum maintainer, instructor, reviewer, and learner	source-quality triangulation and claim-boundary review	source transparency, accountability, and evidence traceability	Official NIST operational technology security guidance.
[of Automation, 2026]	ISA/IEC 62443 Series of Standards	source_quality	source_anchor	quality_spine	2026-05-21	semiannual	curriculum maintainer, instructor, reviewer, and learner	source-quality triangulation and claim-boundary review	source transparency, accountability, and evidence traceability	Official ISA overview of industrial automation and control security standards.
[of the Director of National Intelligence, 2015]	Intelligence Community Directive 203: Analytic Standards	source_quality	source_anchor	quality_spine	2026-05-21	semiannual	curriculum maintainer, instructor, reviewer, and learner	source-quality triangulation and claim-boundary review	source transparency, accountability, and evidence traceability	Official ODNI analytic tradecraft standards directive.
[Union, 2024]	Regulation (EU) 2024/1689: Artificial Intelligence Act	source_quality	source_anchor	quality_spine	2026-05-21	semiannual	curriculum maintainer, instructor, reviewer, and learner	source-quality triangulation and claim-boundary review	source transparency, accountability, and evidence traceability	Official EU Artificial Intelligence Act legal text.
[Cybersecurity and Agency, 2024b]	Preparing for and Mitigating Foreign Influence Operations	source_quality	source_anchor	quality_spine	2026-05-21	semiannual	curriculum maintainer, instructor, reviewer, and learner	source-quality triangulation and claim-boundary review	source transparency, accountability, and evidence traceability	Official CISA guidance on foreign influence operations targeting critical infrastructure.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Organization, 2026b]	Countering Information Threats	source_quality	source_quality	source_quality	2026-05-21	semiannual	curriculum maintainer, instructor, reviewer, and learner	source-quality triangulation and claim-boundary review	source transparency, accountability, and evidence traceability	Official NATO counter-information-threat guidance.
[Agency, 2009]	A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis	curriculum_anchor	analytic_tradecraft	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official structured analytic techniques primer for bias checks, alternatives, and warning analysis.
[Agency, 2016]	A Tradecraft Primer: Basic Structured Analytic Techniques	curriculum_anchor	analytic_tradecraft	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Defense intelligence structured-analysis primer for classroom analytic exercises.
[of the Director of National Intelligence, 2026d]	Intelligence Community Directive 206: Sourcing Requirements for Disseminated Analytic Products	curriculum_anchor	analytic_tradecraft	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official sourcing directive for traceability, citations, source descriptors, and source summaries.
[of the Director of National Intelligence, 2026e]	Objectivity and IC Analytic Standards	curriculum_anchor	analytic_tradecraft	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official ODNI explanation of analytic objectivity, ombuds, and tradecraft standards.
[of State, 2024]	Open Source Intelligence Strategy	curriculum_anchor	osint_geoint	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official strategy source for lawful OSINT governance, discovery, validation, and dissemination.
[Jr., 2007]	Psychology of Intelligence Analysis	curriculum_anchor	analytic_tradecraft	scholarly_or_primary	2026-06-06	annual	source guide context	bibliography traceability	source guide context	Foundational analytic cognition source for bias, mental models, and structured reasoning.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of the Director of National Intelligence, 2026c]	Intelligence Community Directive 204: National Intelligence Priorities Framework	curriculum_anchor	collection_management	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official prioritization directive for translating national intelligence priorities into collection, analysis, risk management, and responsiveness evaluation.
[of Staff, 2026]	JP 2-0: Joint Intelligence	curriculum_anchor	collection_management	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official joint-doctrine landing page for the keystone publication on joint intelligence principles, products, services, and assessments.
[of the Army, 2020]	ATP 2-33.4: Intelligence Analysis	curriculum_anchor	analytic_tradecraft	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official Army analytic doctrine for intelligence-analysis process, structured analytic techniques, analytic design, and cognitive discipline.
[Counterintelligence and Center, 2024]	The National Counterintelligence Strategy	curriculum_anchor	counterintelligence	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official strategy for defensive CI integration, foreign-intelligence threat awareness, strategic advantage protection, and future readiness.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of the Director of National Intelligence and Agency, 2024]	The INT of First Resort: The IC OSINT Strategy 2024-2026	curriculum_anchor	geoint	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official IC OSINT strategy for professionalizing OSINT, integrated collection management, open-source sharing, innovation, and tradecraft.
[Agency, 2026c]	NGA Strategy	curriculum_anchor	geoint	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official NGA strategy anchor for GEOINT readiness, warning, partnership resilience, resource stewardship, and AI integration.
[Archives and Administration, 1981]	Executive Order 12333: United States Intelligence Activities	curriculum_anchor	legal_oversight	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official legal anchor for intelligence authorities, rights-aware collection, analytic competition, oversight, and source-method protection.
[Agency, 2026g]	Foreign Intelligence Surveillance Act	curriculum_anchor	legal_oversight	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official NSA public explanation of FISA oversight for signals intelligence collection governed by statutory and court-authorized controls.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Community, 2026]	How the IC Works	curriculum_anchor	governed_intelligence	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official public explanation of the intelligence cycle, collection disciplines, dissemination, evaluation, oversight, and partners.
[Community, 2020b]	Principles of Artificial Intelligence Ethics for the Intelligence Community	curriculum_anchor	ai_ethics_data_governance	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official IC principles for lawful, accountable, objective, human-centered, secure, resilient, and science-informed AI.
[Community, 2020a]	Artificial Intelligence Ethics Framework for the Intelligence Community	curriculum_anchor	ai_ethics_data_governance	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official IC framework for AI goals, authorities, human judgment, bias mitigation, testing, documentation, explainability, and review.
[of the Director of National Intelligence, 2025b]	Intelligence Community Directive 505: Artificial Intelligence	curriculum_anchor	ai_ethics_data_governance	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official IC AI governance directive covering CAIO roles, oversight, interoperability, civil-liberties review, training data, and impact assessment.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of the Director of National Intelligence, 2025a]	Intelligence Community Directive 504: Intelligence Community Data Management	curriculum_anchor	ethics_data_governance	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official IC data-management directive for data governance, data stewardship, CDO authority, interoperability, and data lifecycle management.
[of the Director of National Intelligence, 2026b]	Authorized Classification and Control Markings Register	curriculum_anchor	governed_intelligence	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official CAPCO register for classification and control-marking vocabulary, abbreviations, portion markings, and dissemination syntax.
[Privacy and Board, 2026]	Oversight Reports	curriculum_anchor	legal_oversight	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official oversight-report library for privacy, civil-liberties, surveillance, watchlisting, facial-recognition, and redress analysis.
[General Services Administration et al., 2026]	Federal Data Strategy	curriculum_anchor	ethics_data_governance	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official federal data-governance benchmark for data as a strategic asset, ethical governance, lifecycle practices, and learning culture.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Agency, 2026a]	Center for the Study of Intelligence	curriculum_anchor	historical_declassified_primary	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official CSI landing page for Studies in Intelligence, declassified professional reflection, analytic history, and institutional learning.
[Agency, 2026h]	NSA Historical Releases	curriculum_anchor	historical_declassified_primary	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official declassified historical-release library for cryptologic history, SIGINT history, COMSEC, oral histories, and historical cases.
[Office, 2026a]	Declassified NRO Programs and Projects	curriculum_anchor	historical_declassified_primary	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official declassified satellite-reconnaissance program archive for CORONA, GAMBIT, POPPY, QUILL, and other historical technical-intelligence cases.
[Archives and Administration, 2026b]	Records of the Central Intelligence Agency	curriculum_anchor	historical_declassified_primary	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official NARA guide to CIA Record Group 263, archival provenance, record series, and declassified intelligence research pathways.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Network, 2026a]	FinCEN Alerts, Advisories, Notices, Bulletins, and Fact Sheets	curriculum_anchor	financial_economic_security	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official FININT source for AML/CFT advisories, typology awareness, sanctions-evasion warnings, red flags, and compliance-oriented monitoring.
[of Foreign Assets Control, 2026]	Sanctions Programs and Country Information	curriculum_anchor	financial_economic_security	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official OFAC sanctions-program library for understanding legal program structure, list maintenance, and compliance-oriented economic statecraft.
[Force, 2025]	The FATF Recommendations	curriculum_anchor	financial_economic_security	international_standard	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official international AML/CFT/CPF standard for risk-based controls, beneficial ownership, information sharing, supervision, and mutual evaluation.
[of Industry and Security, 2026]	Export Enforcement	curriculum_anchor	financial_economic_security	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official export-control enforcement source for compliance, screening, red flags, voluntary disclosures, and national-security protection of sensitive items.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Authority, 2026]	Model AI Governance Framework for Agentic AI	curriculum_anchor	agentic_ai_governance	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Government framework focused on agentic AI delegation, controls, and safe deployment.
[ASD ACSC and NCSC-UK, 2026]	Careful Adoption of Agentic AI Services	curriculum_anchor	agentic_ai_governance	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Joint government guidance for deploying agentic AI with identity, logging, and progressive controls.
[of Standards and Technology, 2026a]	Accelerating the Adoption of Software and Artificial Intelligence Agent Identity and Authorization	curriculum_anchor	agentic_ai_governance	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	NIST concept paper for applying identity and authorization standards to software and AI agents.
[of Standards and Technology, 2026c]	AI Agent Standards Initiative	curriculum_anchor	agent_interoperability	official_primary	2026-06-11	quarterly	standards steward, agent architect, assurance reviewer, procurement assessor, instructor, and learner	agent standards crosswalk, secure delegation review, identity evidence, interoperability claims, and evaluation-scope caveats	secure delegated action, accountable non-human identity, interoperability, least-privilege user control, and auditable agent behavior	Official NIST initiative for trusted, interoperable, and secure AI-agent standards, protocols, identity, and evaluation research.
[UK Department for Science et al., 2024]	AI Safety Institute Approach to Evaluations	curriculum_anchor	agentic_ai_governance	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official evaluation guidance for advanced AI systems, including agent evaluations for tool use, semi-autonomy, and real-world actions.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Project, 2026b]	OWASP Top 10 for Agentic Applications for 2026	curriculum_anchor	agentic_ai_security	security_standard	2026-06-11	semiannual	security architect, red-team reviewer, release owner, instructor, and learner	agentic application risk taxonomy, tool-misuse review, identity-and-privilege checks, supply-chain checklist, and secure-release gate evidence	security, least privilege, supply-chain integrity, safe tool use, accountable agent behavior, and harm prevention	OWASP GenAI Security Project resource identifying critical risks and mitigations for autonomous and agentic AI applications.
[MITRE, 2026a]	MITRE ATLAS	curriculum_anchor	red_team_research	research_standard	2026-06-11	quarterly	AI security analyst, red-team reviewer, incident responder, instructor, and learner	adversarial-AI threat taxonomy, defensive red-team mapping, AI control coverage, and incident-response exercise scoping	security, accountable defensive testing, risk communication, incident readiness, and harm prevention	MITRE ATLAS is a living knowledge base for adversarial threats to AI-enabled systems, useful for defensive red-team mapping and control coverage.
[Project, 2025d]	OWASP Top 10 for Large Language Model Applications	curriculum_anchor	agentic_ai_governance	security_standard	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Security taxonomy for prompt injection, excessive agency, data leakage, and LLM application risks.
[of Standards and Technology, 2022d]	Secure Software Development Framework, NIST SP 800-218	curriculum_anchor	agentic_ai_governance	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official secure development framework for agent tooling, connectors, and software supply chains.
[of Standards and Technology, 2024f]	The NIST Cybersecurity Framework (CSF) 2.0	curriculum_anchor	iot_ot_defense	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official cybersecurity-risk governance framework that adds the Govern function and supplies a common language for AI, OT, and enterprise risk.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of Standards and Technology, 2022b]	Engineering Trustworthy Secure Systems, NIST SP 800-160 Vol. 1 Rev. 1	curriculum_anchor	ics_ot_defense	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Systems-security engineering foundation for trustworthy systems in contested operational environments and related training programs.
[of Standards and Technology, 2016]	Guide to Cyber Threat Information Sharing, NIST SP 800-150	curriculum_anchor	cyber_threat_intelligence	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official guidance for establishing threat-information sharing goals, communities, distribution rules, and defensive use of indicators and TTPs.
[of Standards and Technology, 2025c]	Incident Response Recommendations and Considerations, NIST SP 800-61 Rev. 3	curriculum_anchor	cyber_threat_intelligence	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official incident-response profile for preparation, detection, response, recovery, and continuous improvement under CSF 2.0.
[of Standards and Technology, 2022c]	Cybersecurity Supply Chain Risk Management Practices, NIST SP 800-161 Rev. 1	curriculum_anchor	cyber_threat_intelligence	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official supply-chain risk-management guidance for identifying, assessing, and mitigating product, service, vendor, and process risks.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Cybersecurity and Agency, 2026c]	ICS Recommended Practices	curriculum_anchor	ics_ot_defense	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official defensive ICS practice library for defense-in-depth, forensics, incident response, and remote access.
[Cybersecurity and Agency, 2026f]	CISA Tabletop Exercise Packages	curriculum_anchor	ics_ot_defense	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official exercise packages for cyber, physical, ICS, ransomware, and convergence tabletop scenarios.
[of Standards and Technology, 2006]	Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities	curriculum_anchor	ics_ot_defense	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official methodology for designing, conducting, and evaluating test, training, and exercise programs.
[MITRE, 2026c]	MITRE ATT&CK for ICS Matrix	curriculum_anchor	ics_ot_defense	research_standard	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Threat-informed defensive matrix for ICS tactics and techniques, used for coverage mapping.
[for Security Policy, 2025]	Enhancing Cognitive Security and Societal Resilience to Counter Cognitive Warfare	curriculum_anchor	cognitive_influence_security	scholarship_policy	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Policy-scholarship source for cognitive security, information literacy, critical thinking, and whole-of-society resilience.
[NSA and partners, 2025]	Principles for the Secure Integration of Artificial Intelligence in Operational Technology	curriculum_anchor	ics_ot_defense	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Joint government guidance for AI governance, assurance, safety, and security in OT environments.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Foundation, 2026]	Advancing Artificial Intelligence Agent Ecosystems through the NSF PESOSE Program	curriculum_anchor	agentic_ai_governance	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official NSF source for open AI-agent protocol ecosystems, interoperability, identity, access control, auditability, and safe message formats.
[for Disease Control and Prevention, 2026]	Considerations for Agentic Research in Public Health	curriculum_anchor	agentic_ai_governance	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official public-health guidance for scoping agentic research, human oversight, expert validation, sensitive-data avoidance, and non-replacement of professional judgment.
[of Standards and Technology, 2026f]	NIST AI RMF Playbook	curriculum_anchor	ai_ethics_data_governance	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official AI RMF playbook for translating Govern, Map, Measure, and Manage functions into curriculum controls and review prompts.
[OECD, 2024]	OECD AI Principles	curriculum_anchor	ai_ethics_data_governance	international_standard	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official OECD principles for human-centered values, robustness, transparency, accountability, and inclusive AI growth.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[for Standardization, 2023b]	ISO/IEC 42001:2023 Artificial Intelligence Management System	curriculum_anchor	ethics_data_governance	international_standard	2026-05-21	annual	source guide context	bibliography traceability	source guide context	International AI management-system standard for responsible AI governance, traceability, transparency, risk, and continual improvement.
[for Standardization, 2023a]	ISO/IEC 23894:2023 Artificial Intelligence Guidance on Risk Management	curriculum_anchor	ethics_data_governance	international_standard	2026-05-21	annual	source guide context	bibliography traceability	source guide context	International guidance for integrating AI-specific risk management into organizational activities, products, systems, and services.
[of Europe, 2024]	Framework Convention on Artificial Intelligence	curriculum_anchor	legal_oversight	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official treaty anchor for human rights, democracy, rule-of-law, risk management, accountability, and public-sector AI governance.
[Office, 2025]	Copyright and Artificial Intelligence, Part 3: Generative AI Training	curriculum_anchor	privacy_ip_governance	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official U.S. copyright policy source for generative-AI training, rights-holder impacts, transparency, licensing, and IP governance.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of Standards and Technology, 2020b]	Zero Trust Architecture, NIST SP 800-207	curriculum_anchor	agentic_ai_governance	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official zero-trust architecture guidance for identity-centric authorization, continuous evaluation, least privilege, and policy enforcement.
[of Standards and Technology, 2025b]	Digital Identity Guidelines, NIST SP 800-63-4	curriculum_anchor	agentic_ai_governance	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official digital-identity guidance for authentication, federation, identity proofing, and agent/tool authorization analogies.
[IETF, 2025]	RFC 9700: Best Current Practice for OAuth 2.0 Security	curriculum_anchor	agentic_ai_governance	internet_standard	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Internet standards-track security guidance for OAuth deployment, token protection, redirect safety, and authorization hardening.
[IETF, 2023]	RFC 9449: OAuth 2.0 Demonstrating Proof of Possession	curriculum_anchor	agentic_ai_governance	internet_standard	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Internet standard for sender-constrained OAuth tokens, useful for agent tool-call identity and credential-binding discussions.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of Standards and Technology, 2012]	Guide for Conducting Risk Assessments, NIST SP 800-30 Rev. 1	curriculum_anchor	legal_oversight	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official risk-assessment method for threat, vulnerability, impact, likelihood, uncertainty, and residual-risk reasoning.
[of Standards and Technology, 2018b]	Risk Management Framework for Information Systems and Organizations, NIST SP 800-37 Rev. 2	curriculum_anchor	legal_oversight	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official RMF lifecycle source for preparation, categorization, control selection, implementation, assessment, authorization, and monitoring.
[of Standards and Technology, 2011a]	Information Security Continuous Monitoring, NIST SP 800-137	curriculum_anchor	cyber_threat_intelligence	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official continuous-monitoring guidance for metrics, status awareness, ongoing authorization, and governance feedback loops.
[of Standards and Technology, 2011b]	Managing Information Security Risk, NIST SP 800-39	curriculum_anchor	legal_oversight	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official enterprise-risk source for mission, organization, and system tiers, risk framing, assessment, response, and monitoring.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of Standards and Technology, 2021]	Enhanced Security Requirements for Protecting Controlled Unclassified Information, NIST SP 800-172	curriculum_anchor	cybersecurity_intelligence	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official enhanced security requirements for high-value CUI, source handling analogies, system integrity, and advanced persistent threat resistance.
[of Standards and Technology, 2022a]	Towards a Standard for Identifying and Managing Bias in Artificial Intelligence	curriculum_anchor	ai_ethics_data_governance	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official NIST source for AI bias concepts, socio-technical framing, measurement limits, and governance-oriented mitigation.
[Committee, 2025]	STIX Version 2.1	curriculum_anchor	cyber_threat_intelligence	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	OASIS CTI standard for expressing cyber threat and observable information with structured objects, relationships, sightings, and markings.
[Committee, 2021]	TAXII Version 2.1	curriculum_anchor	cyber_threat_intelligence	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	OASIS CTI transport standard for defensive threat-intelligence exchange channels, collections, discovery, and API contracts.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[MITRE, 2026b]	MITRE ATT&CK Enterprise Matrix	curriculum_anchor	cyber_threat_intelligence	standard	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Threat-informed enterprise matrix for defensive TTP mapping, coverage analysis, detection engineering, and analytic normalization.
[Cybersecurity and Agency, 2026a]	Cross-Sector Cybersecurity Performance Goals	curriculum_anchor	ics_ot_defense	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official prioritized baseline of IT and OT cybersecurity practices for critical-infrastructure risk reduction and maturity assessment.
[Cybersecurity and Agency, 2026e]	Secure by Design	curriculum_anchor	agentic_ai_governance	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official secure-by-design program source for customer security outcomes, radical transparency, leadership accountability, and safer defaults.
[Cybersecurity and Agency, 2026d]	Known Exploited Vulnerabilities Catalog	curriculum_anchor	cyber_threat_intelligence	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official catalog for prioritizing known exploited vulnerabilities as defensive triage inputs, not as exploitation instructions.
[Agency, 2026b]	GEOINT Artificial Intelligence	curriculum_anchor	geoint	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official NGA source on GEOINT AI, data quality, model performance, interoperability, analyst interaction, and standards leadership.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[for Standardization, 2013]	ISO 19157:2013 Geographic Information - Data Quality	curriculum_anchor	geoint	international_standard	2026-05-21	annual	source guide context	bibliography traceability	source guide context	International geospatial data-quality standard for completeness, logical consistency, positional accuracy, temporal quality, and usability framing.
[Cybersecurity and Agency, 2026b]	Election Security	curriculum_anchor	cognitive_influence	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official CISA election-security source for public-resilience, foreign-influence awareness, rumor control, and defensive communication framing.
[Organization, 2026c]	Countering Hybrid Threats	curriculum_anchor	cognitive_influence	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official NATO source for hybrid-threat resilience across cyber, information, economic, political, and military pressure.
[OECD, 2026c]	Disinformation and Misinformation	curriculum_anchor	cognitive_influence	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official OECD policy source for information integrity, governance responses, public trust, and democratic resilience.
[Network, 2026b]	Beneficial Ownership Information Reporting	curriculum_anchor	financial_economic	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official FinCEN source for beneficial-ownership reporting, entity transparency, exemptions, and compliance-oriented analysis.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of Foreign Assets Control, 2019]	A Framework for OFAC Compliance Commitments	curriculum_anchor	financial_economic_security	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official OFAC compliance framework for management commitment, risk assessment, internal controls, testing, auditing, and training.
[Force, 2021]	Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers	curriculum_anchor	financial_economic_security	international_standard	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official FATF guidance for virtual-asset risk, VASP supervision, travel-rule compliance, and non-evasion FININT education.
[for International Settlements, 2021]	Fintech and the Digital Transformation of Financial Services	curriculum_anchor	financial_economic_security	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official BIS policy source for financial technology, market structure, data, network effects, regulation, privacy, and stability tradeoffs.
[of Standards and Technology, 2017]	Framework for Cyber-Physical Systems: Volume 1, Overview	curriculum_anchor	robot_defense	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official NIST cyber-physical systems framework for functions, timing, trustworthiness, interoperability, and safety-aware architecture.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of Standards and Technology, 2018a]	Protecting Information and System Integrity in Industrial Control System Environments, NIST SP 1800-10	curriculum_anchor	ics_ot_defense	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official NCCoE practice guide for manufacturing-sector ICS integrity, monitoring, architecture, and defensive lab validation.
[Organization, 2026d]	Artificial Intelligence and Intellectual Property	curriculum_anchor	privacy_ip_governance	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official WIPO source for AI and IP policy, training-data rights, copyright infrastructure, transparency, attribution, and member-state dialogue.
[of Standards and Technology, 2026k]	NIST Privacy Framework	curriculum_anchor	privacy_ip_governance	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official privacy risk-management framework for identifying and managing privacy risk, data governance, workforce roles, and enterprise controls.
[of Standards and Technology, 2020a]	Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53 Rev. 5	curriculum_anchor	legal_oversight	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official security and privacy control catalog for control baselines, assessment language, privacy controls, and inherited-control reasoning.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of Standards and Technology, 2024]	Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines, NIST IR 8477	curriculum_anchor	legal_oversight	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official mapping-method source for comparing controls, regulations, frameworks, and guidance without collapsing their separate purposes.
[of Standards and Technology, 2024a]	Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations	curriculum_anchor	agentic_ai_governance	official_primary	2026-05-21	annual	source guide context	bibliography traceability	source guide context	Official adversarial-ML taxonomy for defensive AI threat modeling, mitigation vocabulary, evaluation limits, and safe red-team framing.
[Commission, 2026b]	European AI Office	curriculum_anchor	conformity_and_compliance	official_primary	2026-05-22	quarterly	source guide context	bibliography traceability	source guide context	Official European Commission source for AI Office responsibilities, GPAI oversight, enforcement coordination, codes of practice, and AI Act implementation.
[Commission, 2026h]	General-Purpose AI Code of Practice	curriculum_anchor	conformity_and_compliance	official_primary	2026-05-22	quarterly	source guide context	bibliography traceability	source guide context	Official European Commission source for GPAI Code of Practice drafting, transparency, copyright, safety, security, and AI Act implementation support.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Commission, 2026a]	AI Act	curriculum_anchor	conformity_compliance	official_primary	2026-05-22	quarterly	source guide context	bibliography traceability	source guide context	Official European Commission AI Act implementation page for risk tiers, prohibited practices, GPAI obligations, governance bodies, and phased application.
[for Standardization, 2025]	ISO/IEC 42005:2025 AI System Impact Assessment	curriculum_anchor	conformity_compliance	international_standard	2026-05-22	semiannual	source guide context	bibliography traceability	source guide context	ISO standard page for AI system impact assessment across lifecycle, stakeholder impact documentation, transparency, and accountability.
[for Standardization, 2020]	ISO/IEC TR 24028:2020 Artificial Intelligence Trustworthiness Overview	curriculum_anchor	conformity_compliance	international_standard	2026-05-22	annual	source guide context	bibliography traceability	source guide context	ISO technical report page for AI trustworthiness terminology, approaches, engineering considerations, and governance vocabulary.
[Office, 2021]	Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities	curriculum_anchor	conformity_compliance	official_primary	2026-05-22	annual	source guide context	bibliography traceability	source guide context	Official GAO accountability framework for AI governance, data, performance, monitoring, and accountability evidence.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[UNESCO, 2021]	Recommendation on the Ethics of Artificial Intelligence	curriculum_anchor	human_rights_governance	international_soft_law	2026-05-22	annual	source guide context	bibliography traceability	source guide context	Official UNESCO recommendation source for human rights, fairness, transparency, accountability, education, culture, environment, and governance.
[of the United Nations High Commissioner for Human Rights, 2026a]	Digital Space and Human Rights	curriculum_anchor	human_rights_governance	official_primary	2026-05-22	semiannual	source guide context	bibliography traceability	source guide context	Official OHCHR portal for human rights in digital space, including technology, privacy, civic space, equality, and remedy concerns.
[of the United Nations High Commissioner for Human Rights, 2026b]	The Right to Privacy in the Digital Age	curriculum_anchor	human_rights_governance	official_primary	2026-05-22	semiannual	source guide context	bibliography traceability	source guide context	Official OHCHR privacy-in-the-digital-age page for surveillance, data protection, AI, remedy, and human-rights safeguards.
[of Europe, 2018]	Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data	curriculum_anchor	human_rights_governance	official_primary	2026-05-22	annual	source guide context	bibliography traceability	source guide context	Official Council of Europe source for Convention 108+ privacy, data-protection principles, transborder flows, and supervisory cooperation.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[UNESCO, 2023]	Guidance for Generative AI in Education and Research	curriculum_and_instruction	education_association	official_primary	2026-05-22	annual	source guide context	bibliography traceability	source guide context	Official UNESCO publication for generative AI education governance, assessment integrity, age safeguards, teacher roles, and research use.
[UNESCO, 2024]	AI Competency Frameworks for Teachers and Students	curriculum_and_instruction	education_association	official_primary	2026-05-22	annual	source guide context	bibliography traceability	source guide context	Official UNESCO source for AI competency frameworks supporting teacher development, student capabilities, ethics, and curriculum design.
[Report, 2026]	AI and Education	curriculum_and_instruction	education_association	official_primary	2026-05-22	semiannual	source guide context	bibliography traceability	source guide context	Official UNESCO GEM source hub for AI and education evidence, policy, access, assessment, and equity analysis.
[OECD, 2026b]	Artificial Intelligence in Education	curriculum_and_instruction	education_association	official_primary	2026-05-22	semiannual	source guide context	bibliography traceability	source guide context	Official OECD topic page for AI in education, learning systems, assessment, teacher support, and education policy.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Commission, 2026g]	Digital Education Action Plan 2021-2027	curriculum_and_assessment	education_ministry	official_primary	2026-05-22	semiannual	source guide context	bibliography traceability	source guide context	Official European Commission source for digital education policy, digital skills, AI in education, teacher capacity, and assessment readiness.
[Observatory, 2026b]	AI in the Public Sector	curriculum_and_assessment	public_sector_digital_transformation	official_primary	2026-06-06	semiannual	source guide context	bibliography traceability	source guide context	Official OECD.AI source for public-sector AI adoption, governance, public value, accountability, and government service transformation.
[GovTech and Team, 2026]	Artificial Intelligence Working Group	curriculum_and_assessment	public_sector_digital_transformation	official_primary	2026-05-22	semiannual	source guide context	bibliography traceability	source guide context	Official World Bank GovTech source for public-sector AI policy instruments, implementation knowledge exchange, and inclusive government capacity.
[Bank, 2026]	GovTech: Putting People First	curriculum_and_assessment	public_sector_digital_transformation	official_primary	2026-05-22	semiannual	source guide context	bibliography traceability	source guide context	Official World Bank GovTech program source for digital public infrastructure, citizen engagement, core systems, and public-sector modernization.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Administration, 2026]	AI Guide for Government	curriculum_anchor	public_sector_practice	official_primary	2026-05-22	quarterly	source guide context	bibliography traceability	source guide context	Official U.S. government AI resource hub for agency adoption, responsible use, policy references, and public-sector implementation support.
[Commission, 2026e]	European Data Governance Act	curriculum_anchor	cross_border_data_spaces	official_primary	2026-05-22	semiannual	source guide context	bibliography traceability	source guide context	Official European Commission source for data-sharing trust, data intermediaries, public-sector data reuse, data altruism, and European Data Spaces.
[Commission, 2026d]	Data Act Explained	curriculum_anchor	cross_border_data_spaces	official_primary	2026-05-22	semiannual	source guide context	bibliography traceability	source guide context	Official European Commission source explaining Data Act access, use, connected-product data, interoperability, and cross-sector data availability.
[Commission, 2026c]	Common European Data Spaces	curriculum_anchor	cross_border_data_spaces	official_primary	2026-05-22	semiannual	source guide context	bibliography traceability	source guide context	Official European Commission source for Common European Data Spaces, single-market data governance, cross-domain infrastructures, and interoperability specifications.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Commission, 2026f]	A European Strategy for Data	curriculum_anchor	cross_border_official_primary	official_primary	2026-05-22	semiannual	source guide context	bibliography traceability	source guide context	Official European Commission strategy source for single-market data, data sovereignty, common data spaces, and rights-preserving innovation.
[Consortium, 2023a]	Web of Things (WoT) Architecture 1.1	curriculum_anchor	agent_interoperability_standards	standards_primary	2026-05-22	annual	source guide context	bibliography traceability	source guide context	W3C Recommendation for Web of Things architecture, thing models, security considerations, interoperability, and application patterns.
[Consortium, 2023c]	Web of Things (WoT) Thing Description 1.1	curriculum_anchor	agent_interoperability_standards	standards_primary	2026-05-22	annual	source guide context	bibliography traceability	source guide context	W3C Recommendation for machine-readable thing descriptions, interaction affordances, metadata, security, and protocol bindings.
[Consortium, 2023b]	Web of Things (WoT) Discovery	curriculum_anchor	agent_interoperability_standards	standards_primary	2026-05-22	annual	source guide context	bibliography traceability	source guide context	W3C Recommendation for discovering Web of Things resources using directories, metadata, privacy, and security considerations.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Initiative, 2026b]	OpenAPI Specification	curriculum_anchor	agent_interoperability_standards	standard	2026-05-22	semiannual	source guide context	bibliography traceability	source guide context	Official OpenAPI specification index for describing HTTP APIs, schemas, operations, errors, and contract validation.
[Consortium, 2025b]	Verifiable Credentials Data Model v2.0	curriculum_anchor	agent_interoperability_standards	standard	2026-05-22	annual	source guide context	bibliography traceability	source guide context	W3C Recommendation for verifiable credentials, issuers, holders, verifiers, security, privacy, internationalization, and accessibility considerations.
[Consortium, 2022]	Decentralized Identifiers (DIDs) v1.0	curriculum_anchor	agent_interoperability_standards	standard	2026-05-22	annual	source guide context	bibliography traceability	source guide context	W3C Recommendation for decentralized identifiers, DID documents, verification methods, service endpoints, privacy, and security considerations.
[Force, 2022]	RFC 9110: HTTP Semantics	curriculum_anchor	agent_interoperability_standards	standard	2026-05-22	annual	source guide context	bibliography traceability	source guide context	IETF standard for HTTP semantics used to ground API contracts, methods, status codes, content negotiation, and safe integration language.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Organization, 2026a]	Artificial Intelligence	curriculum_anchor	workforce_governance	official_primary	2026-05-22	semiannual	source guide context	bibliography traceability	source guide context	Official ILO topic page for AI and work, digital transformation, occupational impact, skills, safety, and social dialogue.
[Organization and Nations, 2024]	Mind the AI Divide: Shaping a Global Perspective on the Future of Work	curriculum_anchor	workforce_governance	official_primary	2026-05-22	annual	source guide context	bibliography traceability	source guide context	Official ILO/UN publication on uneven AI adoption, labour-market exposure, global equity, fairness, and social justice.
[Organization, 2019]	Global Commission on the Future of Work	curriculum_anchor	workforce_governance	official_primary	2026-05-22	annual	source guide context	bibliography traceability	source guide context	Official ILO source for a human-centred future-of-work agenda, lifelong learning, labour guarantees, social protection, and decent work.
[Observatory, 2026a]	AI and Work	curriculum_anchor	workforce_governance	official_primary	2026-06-06	semiannual	source guide context	bibliography traceability	source guide context	Official OECD.AI source for AI, work, labour-market transitions, skills, productivity, workplace governance, and policy responses.
[Consortium, 2013b]	PROV Overview	curriculum_anchor	model_data_interchange	international_standard	2026-05-22	annual	source guide context	bibliography traceability	source guide context	W3C Recommendation overview for provenance interchange, entities, activities, agents, and provenance-family specifications.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Consortium, 2013a]	PROV-O: The PROV Ontology	curriculum_anchor	model_data_interop	international_standard	2026-06-22	annual	source guide context	bibliography traceability	source guide context	W3C Recommendation for the PROV ontology supporting machine-readable provenance relationships among entities, activities, agents, and roles.
[Consortium, 2024]	Data Catalog Vocabulary (DCAT) Version 3	curriculum_anchor	model_data_interop	international_standard	2026-06-22	annual	source guide context	bibliography traceability	source guide context	W3C Recommendation for cataloging datasets and data services with metadata, distributions, provenance, access, and quality signals.
[Consortium, 2017]	Data on the Web Best Practices	curriculum_anchor	model_data_interop	international_standard	2026-06-22	annual	source guide context	bibliography traceability	source guide context	W3C Recommendation for publishing data with metadata, licenses, provenance, quality, versioning, identifiers, and machine-readable formats.
[of Standards and Technology, 2026h]	NIST Big Data Interoperability Framework	curriculum_anchor	model_data_interop	official_primary	2026-06-06	annual	source guide context	bibliography traceability	source guide context	Official NIST program source for big-data interoperability, reference architecture, data interfaces, vocabulary, and technology roadmap.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[DataCite, 2026]	DataCite Metadata Schema	curriculum_architect	model_data_provenance	technical_standard	2026-05-22	annual	source guide context	bibliography traceability	source guide context	Official DataCite schema source for dataset citation metadata, persistent identifiers, creators, dates, relationships, and versioning.
[for Content Provenance and Authenticity, 2026]	C2PA Specifications	curriculum_architect	model_data_provenance	technical_standard	2026-06-06	semiannual	source guide context	bibliography traceability	source guide context	C2PA specifications source for content credentials, provenance manifests, assertions, signing, verification, and media authenticity evidence.
[Initiative, 2026c]	WCAG 2 Overview	curriculum_architect	accessibility_digital_inclusion	standard	2026-05-22	semiannual	learner, instructor, public-sector service user, and accessibility reviewer	accessibility acceptance criteria and remediation evidence	disability access, equal participation, and digital inclusion	W3C WAI overview for WCAG 2.0, 2.1, and 2.2 conformance, success criteria, and accessibility standard selection in digital curriculum artifacts.
[CAST, 2024]	CAST Universal Design for Learning Guidelines version 3.0	curriculum_architect	accessibility_digital_inclusion	guideline	2026-05-22	annual	learner, instructor, accommodation reviewer, and curriculum steward	UDL review checklist and inclusive-assessment evidence	accessibility, inclusion, learner agency, and educational equity	CAST UDL Guidelines 3.0 source for designing multiple means of engagement, representation, action, expression, and learner agency.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of Justice, 2024]	Fact Sheet: New Rule on the Accessibility of Web Content and Mobile Apps Provided by State and Local Governments	curriculum_author	accessibility_official	official_primary	2026-05-22	quarterly	public entity, contractor, learner, disabled service user, and compliance reviewer	public-sector accessibility gate and vendor deliverable review	disability rights, equal access, and public-service inclusion	DOJ ADA Title II fact sheet for state and local government web and mobile app accessibility obligations, WCAG technical standard use, contractors, and compliance timing.
[Board, 2026]	What is a Data Protection Impact Assessment and When Is This Mandatory?	curriculum_author	rights_impact_officer	privacy_primary	2026-05-22	semiannual	data controller, data subject, instructor, reviewer, and privacy officer	DPIA trigger worksheet and mitigation record	privacy, data protection, automated-decision safeguards, and redress	EDPB data-protection guide entry defining DPIA use for planned processing, high-risk processing, automated evaluation, sensitive data, and systematic monitoring.
[Board, 2018]	Endorsed WP29 Guidelines	curriculum_author	rights_impact_officer	privacy_primary	2026-05-22	semiannual	privacy officer, legal reviewer, instructor, and learner	verified DPIA reference and source-refresh evidence	privacy, data protection, transparency, and accountable processing	EDPB list of endorsed WP29 GDPR guidelines, including DPIA guidance for processing likely to result in a high risk.
[OECD, 2015]	Recommendation of the Council on Public Procurement	curriculum_author	procurement_official	vendor_primary	2026-05-22	annual	public buyer, vendor, contract manager, auditor, and affected public	vendor oversight gate, procurement evidence register, and contract-review checklist	public accountability, fairness, transparency, and anti-corruption safeguards	OECD public procurement legal instrument for transparency, integrity, access, risk management, accountability, evaluation, and supplier participation.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Partnership, 2026]	Open Contracting Data Standard	curriculum_anchor	procurement_technical_standard	official_primary	2026-05-22	annual	procurement analyst, auditor, vendor, civic reviewer, and instructor	contracting data schema and vendor record provenance check	public transparency, accountability, anti-corruption, and access to information	International open data standard for publishing public contracting data and documents across planning, tender, award, contract, and implementation stages.
[of Standards and Technology, 2025d]	Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile	curriculum_anchor	agent_incident_response	official_primary	2026-05-22	semiannual	incident commander, system steward, instructor, learner, and risk owner	agent incident response drill and escalation evidence	resilience, accountability, due care, and harm minimization	NIST SP 800-61 Rev. 3 source for integrating incident response with risk management, preparation, detection, response, and recovery.
[for Cybersecurity, 2020]	Artificial Intelligence Cybersecurity Challenges	curriculum_anchor	red_team_assurance	official_primary	2026-05-22	annual	security reviewer, vendor assessor, instructor, and system steward	AI threat-model critique and red-team assurance checklist	secure AI, data protection, trustworthiness, and supply-chain accountability	ENISA AI cybersecurity report mapping AI lifecycle assets, threat landscape, supply-chain concerns, security controls, and data-protection needs.
[of Standards and Technology, 2026g]	AI Research: Security and Resilience	curriculum_anchor	red_team_assurance	official_primary	2026-05-22	quarterly	red-team reviewer, assurance lead, instructor, and learner	adversarial assurance cycle and mitigation evidence	security, reliability, harm prevention, and accountable AI testing	NIST AI security and resilience research hub for secure-and-resilient AI trustworthiness, adversarial machine learning taxonomy, and mitigation work.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of Standards and Technology, 2026d]	NIST AI Resource Center	curriculum_anchor	technical_standard	official_primary	2026-05-22	quarterly	assurance lead, instructor, compliance reviewer, and learner	TEVV evidence plan and AI RMF crosswalk	trustworthy AI, accountability, safety, and rights-preserving evaluation	NIST AI Resource Center source for AI RMF operationalization, playbook resources, crosswalks, profiles, and testing, evaluation, verification, and validation support.
[OECD, 2017]	Recommendation of the Council on Open Government	curriculum_anchor	public_sector_transparency	official_primary	2026-05-22	annual	public official, civic reviewer, instructor, affected community, and learner	public transparency statement and stakeholder-review evidence	access to information, participation, accountability, and democratic governance	OECD open government legal instrument for transparency, integrity, accountability, stakeholder participation, civic space, and public-sector disclosure.
[Consortium, 2025a]	Verifiable Credential Data Integrity 1.0	curriculum_anchor	model_data_provenance	technical_standard	2026-05-22	semiannual	data steward, verifier, instructor, learner, and provenance auditor	data lineage registry and verifiable-evidence check	data integrity, provenance, authenticity, and accountable reuse	W3C Recommendation for data integrity proofs, proof sets, proof chains, verification methods, and transformed data protection in verifiable credentials.
[Margaret Mitchell and Gebru, 2019]	Model Cards for Model Reporting	curriculum_anchor	model_card_scholarship	scholarly	2026-05-22	annual	model steward, assurance reviewer, instructor, learner, and affected user	model card review and model-release evidence packet	transparency, fairness, informed use, contestability, and accountable deployment	Scholarly source for documenting intended use, evaluation procedures, benchmarked performance, limitations, and model-release context.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Timnit Gebru and Crawford, 2021]	Datasheets for Datasets	curriculum_author	dataset_documentation	scholarly_primary	2026-05-22	annual	data steward, dataset creator, instructor, learner, and downstream reviewer	dataset datasheet review and data lineage registry	data transparency, accountable reuse, bias review, privacy, and affected-group visibility	Scholarly source for dataset documentation covering motivation, composition, collection process, recommended uses, communication, transparency, and accountability.
[Service, 2025b]	Algorithmic Transparency Recording Standard Hub	curriculum_author	algorithmic_transparency_reporting	official_primary	2026-05-22	quarterly	public official, transparency reviewer, instructor, affected community, and learner	transparency notice workflow and public accountability evidence	access to information, public accountability, participation, privacy, and civic trust	Official UK hub for ATRS records, public-sector transparency expectations, mandatory-scope policy, template guidance, and publication support.
[Service, 2025a]	Guidance for Organisations Using the Algorithmic Transparency Recording Standard	curriculum_author	algorithmic_transparency_reporting	official_primary	2026-05-22	quarterly	public official, records steward, instructor, transparency reviewer, and learner	transparency notice field checklist and publication decision evidence	public transparency, explainability, accessibility, data protection, and redress	Official guidance for completing and publishing ATRS records, including public-sector template support and repository submission expectations.
[of Standards and Technology, 2024a]	Secure Software Development Practices for Generative AI and Dual-Use Foundation Models	curriculum_author	secure_release_governance	official_primary	2026-05-22	semiannual	system steward, security reviewer, vendor assessor, instructor, and learner	release and change-control gate with secure-development evidence	security, resilience, due care, accountability, and harm prevention	NIST SSDF Community Profile for AI model development, AI systems using models, AI system acquisition, and secure lifecycle practices.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Board, 2017]	Revised 508 Standards and 255 Guidelines	curriculum_anchor	learner_support	official_primary	2026-05-22	semiannual	learner, instructor, accessibility reviewer, procurement reviewer, and public-service owner	accommodation plan, accessibility remediation log, and alternative-means decision	accessibility, equal participation, public-service access, and reasonable accommodation	Official ICT accessibility standards for federal information and communication technology, including procurement, development, maintenance, use, exceptions, and documentation.
[of Standards and Technology, 2025a]	Assessing Risks and Impacts of AI (ARIA): Pilot Evaluation Report	curriculum_anchor	assurance_evaluation	official_primary	2026-05-22	quarterly	assurance lead, evaluator, instructor, learner, and affected user	agent evaluation protocol and adversarial assurance evidence	validity, reliability, safety, fairness, user impact, and accountable testing	NIST ARIA pilot report describing evaluation scenarios, model testing, red teaming, field testing, dialogue annotation, tester questionnaires, and measurement trees.
[Archives and Administration, 2026a]	Inventory of NARA Artificial Intelligence (AI) Use Cases	curriculum_anchor	records_retention	official_primary	2026-05-22	quarterly	records officer, public official, instructor, transparency reviewer, and learner	AI use-case inventory review and records-audit trail	records access, public transparency, privacy, archival integrity, and FOIA accountability	Official NARA inventory of current and planned AI use cases, including production, pilot, and planned AI applications tied to records, discovery, FOIA, and archival access.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of the President, 2025a]	M-25-21: Accelerating Federal Use of AI through Innovation, Governance, and Public Trust	curriculum_anchor	risk_exception	official_primary	2026-05-22	quarterly	agency AI officer, risk owner, instructor, oversight reviewer, and learner	risk exception memo and agency AI governance crosswalk	public trust, privacy, security, accessibility, transparency, and accountable governance	OMB memorandum for federal AI strategies, AI maturity, data traceability, continuous monitoring, governance, privacy, security, workforce, and public trust.
[of the President, 2025b]	M-25-22: Driving Efficient Acquisition of Artificial Intelligence in Government	curriculum_anchor	procurement_oversight	official_primary	2026-05-22	quarterly	procurement official, vendor assessor, instructor, system steward, and learner	procurement oversight loop and vendor-performance monitoring packet	transparent acquisition, vendor accountability, public value, interoperability, and due care	OMB memorandum for federal AI acquisition, product demonstrations, performance-based requirements, Quality Assurance Surveillance Plans, monitoring, and transparency requirements.
[of Standards and Technology, 2024e]	Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile	curriculum_anchor	assurance_evaluation	official_primary	2026-06-11	semiannual	AI governance lead, assurance reviewer, instructor, system steward, procurement assessor, and learner	AI risk profile crosswalk, generative-AI evaluation evidence, misuse-risk review, and source-backed trustworthiness caveats	trustworthy AI, safety, security, privacy, fairness, transparency, accountability, and documented evaluation limits	NIST AI 600-1 profile for generative AI risk management, risk framing, evaluation actions, misuse considerations, and AI RMF alignment.
[Cybersecurity and Agency, 2024a]	AI Red Teaming: Applying Software TEVV for AI Evaluations	curriculum_anchor	red_team_oversight	official_primary	2026-05-22	semiannual	red-team reviewer, evaluator, critical-infrastructure steward, instructor, and learner	AI red-team TEVV crosswalk and assurance critique	safety, security, fit-for-purpose evaluation, reliability, and accountable testing	CISA guidance connecting AI red teaming to testing, evaluation, verification, and validation for security and safety assurance.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Cybersecurity et al., 2025b]	AI Data Security: Best Practices for Securing Data Used to Train and Operate AI Systems	curriculum_anchor	model_data_provenance	official_primary	2026-06-11	semiannual	data steward, model owner, procurement reviewer, release reviewer, instructor, and learner	model/data provenance card, AI data-security control review, training-data integrity checks, operational-data lifecycle mapping, and release-readiness evidence	data integrity, confidentiality, provenance, privacy, trusted infrastructure, accountable reuse, and trustworthy AI outcomes	Joint official cybersecurity information sheet on best practices for securing data used to train and operate AI systems across the lifecycle.
[of Standards and Technology, 2026e]	Concept Note: AI RMF Profile on Trustworthy AI in Critical Infrastructure	curriculum_anchor	assurance_evaluation	official_primary	2026-05-22	quarterly	critical-infrastructure steward, OT defender, assurance reviewer, instructor, and learner	critical-infrastructure AI RMF profile crosswalk and tabletop assurance review	safety, resilience, reliability, security, public service continuity, and accountable infrastructure governance	NIST concept note for a critical-infrastructure AI RMF profile covering AI-enabled IT, OT, and industrial-control environments.
[for Economic Co-operation and Development, 2025b]	Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions	curriculum_anchor	public_sector_transparency	official_primary	2026-05-22	semiannual	public-sector steward, policy reviewer, service designer, instructor, and learner	public-sector AI guardrail and transparency crosswalk	public trust, accountability, transparency, inclusion, service quality, and citizen-facing safeguards	OECD public-sector AI governance report framing enablers, guardrails, and engagement for trustworthy AI in government.
[Archives and Administration, 2025]	NARA 2025 AI Compliance Plan	curriculum_anchor	records_retention	official_primary	2026-05-22	semiannual	records officer, public-sector AI steward, compliance reviewer, instructor, and learner	records-retention and AI compliance audit trail	public records, transparency, auditability, privacy-by-design, accountability, and public trust	NARA plan for AI governance, public trust, audits, records-aware AI use, transparency, and compliance with federal AI policy.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of Canada Secretariat, 2026a]	Guide on the Use of Agentic Artificial Intelligence	curriculum_anchor	public_sector_official_training	primary	2026-05-24	quarterly	public-sector AI steward, service owner, instructor, learner, and oversight reviewer	bounded-autonomy run card, recoverability review, approval threshold, monitoring evidence, and public-sector service assurance	public trust, accountability, transparency, privacy, accessibility, human review, and service fairness	Government of Canada guide for accountable public-sector use of agentic AI, including governance, risk, transparency, testing, monitoring, and human oversight considerations.
[of Canada Secretariat, 2026b]	Algorithmic Impact Assessment tool	curriculum_anchor	rights_impact_assessment	primary	2026-05-24	quarterly	AI program owner, privacy reviewer, rights-impact assessor, instructor, and learner	algorithmic impact worksheet, rights-risk triage, mitigation evidence, and review threshold	privacy, equality, procedural fairness, redress, transparency, accessibility, and affected-group review	Government of Canada Algorithmic Impact Assessment tool for structured impact-level scoring, mitigation planning, and accountable review of automated decision systems.
[of Canada Secretariat, 2025]	Canada launches first register of AI uses in federal government	curriculum_anchor	public_sector_official_training	primary	2026-05-24	quarterly	public official, transparency reviewer, records officer, instructor, and learner	public AI-use inventory review, disclosure checklist, register refresh, and transparency evidence	public transparency, accountability, accessible notice, public trust, privacy, and service-user awareness	Official announcement of Canada's federal AI register, used as a transparency anchor for AI use-case inventories and public-facing disclosure.
[of Canada, 2025]	AI Strategy for the Federal Public Service 2025-2027: Priority areas	curriculum_anchor	workforce_governance	primary	2026-05-24	quarterly	public-sector AI leader, workforce planner, instructor, service steward, and learner	public-sector AI strategy crosswalk, workforce-readiness map, governance maturity review, and implementation evidence	public value, accountable service delivery, workforce capability, inclusion, transparency, and trust	Government of Canada AI Strategy priority-area page for public-service AI adoption, governance, people, public value, and responsible implementation.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[for Economic Co-operation and Development, 2026b]	AI risks and incidents	curriculum_anchor	agent_incidents	official_primary	2026-05-24	quarterly	incident reviewer, AI risk owner, instructor, policy analyst, and learner	AI incident monitor review, risk pattern briefing, incident taxonomy, and debrief evidence	safety, security, privacy, discrimination, accountability, workplace rights, and public trust	OECD topic page on AI risks and incidents, including AI incident monitoring, hazard evidence, and the need for common incident reporting.
[for Economic Co-operation and Development, 2025a]	Towards a common reporting framework for AI incidents	curriculum_anchor	agent_incidents	official_primary	2026-05-24	quarterly	AI incident lead, assurance reviewer, policy analyst, instructor, and learner	AI incident reporting template, classification checklist, impact review, and lessons-learned loop	safety, accountability, impact transparency, redress evidence, cross-border interoperability, and harm learning	OECD policy paper proposing a common AI incident reporting framework for jurisdictions and sectors, including criteria for impact and risk characterization.
[Nations, 2024]	Global Digital Compact	curriculum_anchor	accessibility_digital_inclusion	official_primary	2026-05-24	semiannual	rights reviewer, inclusion lead, instructor, learner, and public-interest steward	digital-inclusion and AI-governance crosswalk, human-rights review, public participation note, and inclusion evidence	human rights, digital inclusion, accessibility, online safety, public participation, equality, and international cooperation	United Nations Global Digital Compact page and adopted compact context for inclusive, rights-based digital cooperation and global AI governance.
[of Standards and Technology, 2026i]	Dioptra	curriculum_anchor	red_team_testbed	official_primary	2026-05-24	quarterly	assurance evaluator, red-team reviewer, instructor, system steward, and learner	AI red-team testbed evidence, reproducible evaluation run, measurement packet, and assurance artifact	trustworthy AI, safety, security, validity, reliability, transparency, and accountable testing	NIST Dioptra test platform for evaluating AI system risks, adversarial robustness, and measurement workflows in controlled settings.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Cybersecurity et al., 2024]	Joint Guidance on Deploying AI Systems Securely	curriculum_anchor	secure_release	official_primary	2026-05-24	semiannual	AI system owner, security reviewer, release manager, instructor, and learner	secure AI deployment gate, change-control review, rollback evidence, monitoring threshold, and incident trigger	security, reliability, safety, accountability, privacy, operational resilience, and public trust	CISA joint guidance for deploying AI systems securely, used as a release/change-control anchor for AI-enabled services.
[Cybersecurity and Agency, 2025b]	Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products	curriculum_anchor	procurement_vendor	official_primary	2026-05-24	semiannual	OT owner, procurement official, vendor assessor, instructor, and learner	OT procurement checklist, vendor security criteria, defensible selection evidence, and lifecycle assurance review	safety, resilience, accountable procurement, vendor transparency, service continuity, and due care	CISA Secure by Demand considerations for OT owners and operators selecting digital products, used for vendor-governance and procurement review.
[Cybersecurity et al., 2025a]	CISA and Partners Release Asset Inventory Guidance to Strengthen Operational Technology Security	curriculum_anchor	records_retention	official_primary	2026-05-24	semiannual	OT asset owner, records reviewer, security engineer, instructor, and learner	OT asset-inventory register, change evidence, owner field review, and auditability packet	safety, service continuity, operational resilience, accountable records, auditability, and change traceability	CISA and partners' asset-inventory guidance for strengthening operational technology security and keeping OT records reviewable.
[Cybersecurity and Agency, 2025a]	Creating and Maintaining a Definitive View of Your Operational Technology (OT) Architecture	curriculum_anchor	assurance_evidence	official_primary	2026-05-24	semiannual	OT architect, assurance reviewer, operator, instructor, and learner	definitive OT architecture record, evidence map, review cadence, change-control packet, and tabletop assurance baseline	safety, availability, operational resilience, accountable architecture evidence, auditability, and defensive readiness	CISA guidance on creating and maintaining a definitive view of OT architecture, used as an assurance-evidence anchor for cyber-physical readiness.

80.8 Bibliography atlas rows: guide keys, curated anchors, and support-source roles {#sec:bibliography-rows} (continued 2)

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of Excellence, 2026]	New CCDCOE Research Reconceptualises Cognitive Warfare	curriculum_anchor	human_rights_governance	official_primary	2026-05-22	semiannual	source guide context	bibliography traceability	source guide context	CCDCOE 2026 research reconceptualising cognitive warfare as a contest over the structures of interpretation and decision-making rather than information content; introduces systemic invariants and cognitive decoherence.
[Agency, 2024a]	Intrinsic Cognitive Security (ICS)	curriculum_anchor	assurance_evaluation	official_primary	2026-05-22	semiannual	assurance evaluator, formal-methods reviewer, instructor, system steward, and learner	formal-methods assurance evidence, cognitive-attack mitigation catalogue, and probabilistic-guarantee review for mixed-reality system design	safety, cognitive integrity, perceptual security, accountable system design, and verifiable assurance	DARPA Intrinsic Cognitive Security (ICS) program applying probabilistic formal methods to guarantee mixed-reality system designs mitigate cognitive attacks; CAMP knowledgebase analog to MITRE CAPEC.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Alliance, 2025a]	Introducing Cognitive Degradation Resilience (CDR): A Framework for Safeguarding Agentic AI Systems from Systemic Collapse	curriculum_anchor	agent_incident_response	official_primary	2026-05-22	quarterly	AI incident lead, resilience reviewer, instructor, system steward, and learner	agent degradation health probes, six-stage drift monitoring, QSAF-BC control mapping, and systemic-collapse incident review	safety, reliability, operational resilience, accountable monitoring, and harm prevention	CSA Cognitive Degradation Resilience (CDR) framework defining a six-stage degradation cascade for agentic AI networks and seven QSAF-BC controls; treated as a defensive evidence-bounded governance anchor.
[Alliance, 2025b]	Agentic AI Threat Modeling Framework: MAE-STRO	curriculum_anchor	red_team_offsec	official_primary	2026-05-22	quarterly	threat modeler, red-team reviewer, instructor, system steward, and learner	seven-layer threat-model worksheet, cross-layer mitigation map, security-agent self-audit, and agentic threat-modeling review	security, accountability, transparency, supply-chain integrity, and trustworthy AI assurance	CSA MAE-STRO seven-layer threat-modeling framework for the full agentic AI stack from foundation model through agent ecosystem, including the vertical security/compliance layer.
[Mandel and Tetlock, 2018]	Correcting Judgment Correctives in National Security Intelligence	curriculum_anchor	education_assessment	scholarly_peer_reviewed	2026-05-22	annual	source guide context	analytic-bias review checklist, noise-versus-bias diagnostic, recalibration evidence, and SAT-validation critique	source guide context	Peer-reviewed Frontiers in Psychology analysis (NIH PMC) on correcting judgment in national security intelligence, identifying neglect of noise and unipolar treatment of bipolar bias in IC debiasing.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[arXiv preprint authors, 2025a]	Agentic AI Security: Threats, Defenses, Evaluation, and Open Challenges	curriculum_anchor	red_team_assurance	scholarly_preprint	2026-05-22	quarterly	red-team reviewer, threat modeler, instructor, system steward, and learner	agentic threat-taxonomy crosswalk, defense-catalog review, evaluation-benchmark map, and open-challenge research log	security, accountability, transparency, and trustworthy AI assurance	arXiv survey on agentic AI security providing a comprehensive threat taxonomy, defense catalog, evaluation review, and governance perspectives; vendor statistics within treated as ESTIMATE.
[Anthropic, 2024]	Building Effective AI Agents	curriculum_anchor	agent_interoperability	frontier_lab_research	2026-05-22	semiannual	source guide context	bibliography traceability	source guide context	Anthropic research guide establishing the canonical workflows-versus-agents taxonomy and composable agentic patterns (prompt chaining, routing, parallelization, orchestrator-workers, evaluator-optimizer).
[DeepMind and Research, 2026]	Architecting Trust in Artificial Epistemic Agents	curriculum_anchor	model_data_provenance	frontier_lab_research	2026-05-22	annual	source guide context	bibliography traceability	source guide context	Google DeepMind arXiv paper defining the epistemic AI agent and proposing demonstrable competence, falsifiability, virtuous behavior, provenance chains, verifier agents, and knowledge sanctuaries.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Lee and Tiwari, 2024]	Prompt Infection: LLM-to-LLM Prompt Injection within Multi-Agent Systems	curriculum_anchor	agent_incident_response	scholarly_primary	2026-05-22	annual	incident reviewer, threat modeler, instructor, system steward, and learner	cross-agent injection threat briefing, propagation-containment review, LLM-tagging defense map, and synthetic infection tabletop	security, integrity, accountability, and harm prevention	arXiv paper documenting self-replicating LLM-to-LLM prompt injection within multi-agent systems; used as a defensive, evidence-bounded counterintelligence anchor with LLM-tagging mitigation.
[arXiv preprint authors, 2025b]	Systems Security Foundations for Agentic Computing	curriculum_anchor	secure_release_change_control	scholarly_primary	2026-05-22	annual	security architect, release reviewer, instructor, system steward, and learner	agentic trusted-computing-base review, dynamic-privilege change-control map, instruction-data separation evidence, and release-gate analysis	security, integrity, least-privilege accountability, and operational resilience	arXiv analysis framing prompt injection as structurally equivalent to dynamic code loading and arguing for dynamic, context-sensitive privilege management in agentic systems.
[Initiative), 2025]	Agentic AI – Threats and Mitigations	curriculum_anchor	red_team_offensive_ai	official_primary	2026-05-22	quarterly	red-team reviewer, threat modeler, instructor, system steward, and learner	agentic threat-model reference, mitigation baseline checklist, red-team scope guide, and ASI-aligned assurance review	security, accountability, transparency, and trustworthy AI assurance	OWASP Agentic Security Initiative threat-model-based reference of emerging agentic AI threats and mitigations; standards-body guidance for defensive curriculum use.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Alliance, 2026]	Securing Autonomous AI Agents	curriculum_anchor	procurement_official	primary	2026-05-22	quarterly	identity governance lead, procurement assessor, instructor, system steward, and learner	agent identity-governance gap review, IAM-readiness assessment, non-human identity inventory, and procurement assurance checklist	security, accountability, least-privilege governance, auditability, and operational resilience	CSA survey on securing autonomous AI agents quantifying the identity-governance gap; readiness percentages treated as ESTIMATE for curriculum discussion.
[Initiative, 2026a]	CSA Research Note: NIST AI Agent Red-Teaming Standards (March 2026)	curriculum_anchor	red_team_official	primary	2026-05-22	quarterly	red-team reviewer, assurance evaluator, instructor, compliance officer, and learner	AI red-team standards crosswalk, adversarial-ML test scope, multi-attempt evaluation plan, and enterprise compliance review	security, accountability, validity, reliability, transparency, and trustworthy AI assurance	CSA research note on NIST AI agent red-teaming standards summarizing CAISI findings and recommended adversarial-ML testing protocols; reported success-rate figures treated as ESTIMATE.
[United Nations University, 2026]	Why Agentic AI Needs Boundaries Before Freedom	curriculum_anchor	human_rights_official	governance	2026-05-22	semiannual	AI governance steward, oversight reviewer, instructor, policy analyst, and learner	bounded-autonomy boundary review, minimum-necessary-privilege checklist, oversight-and-accountability map, and governance-design rationale	accountability, public trust, human oversight, institutional values alignment, and harm prevention	UNU Macau policy analysis arguing agentic AI requires boundaries before freedom — minimum necessary privilege, delimited scope, sandboxes, explicit permissions, and accountable oversight.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of Standards and Technology, 2024b]	Reducing Risks Posed by Synthetic Content: An Overview of Technical Approaches to Digital Content Transparency	curriculum_anchor	model_data_provenance	official_primary	2026-06-11	annual	provenance reviewer, model-card steward, synthetic-media evaluator, instructor, learner, and affected-person representative	bibliography traceability	transparency, provenance, disclosure, privacy, child safety, non-consensual intimate imagery prevention, and accountable synthetic-media governance	NIST AI 100-4 report on reducing risks posed by synthetic content through digital content transparency, provenance, labeling, watermarking, detection, testing, auditing, and maintenance approaches.
[of Standards and Technology, 2024c]	A Plan for Global Engagement on AI Standards	curriculum_anchor	conformity_compliance	official_primary	2026-06-06	annual	standards lead, compliance reviewer, procurement assessor, instructor, and learner	bibliography traceability	accountability, interoperability, standards participation, transparency, and cross-border governance consistency	NIST AI 100-5 plan for global engagement on AI standards, used to ground standards coordination and cross-jurisdiction AI-governance discussions without claiming a single universal compliance regime.
[U.S. AI Safety Institute and Technology, 2024]	Managing Misuse Risk for Dual-Use Foundation Models, NIST AI 800-1 Initial Public Draft	curriculum_anchor	red_team_misuse	official_draft	2026-06-06	quarterly	AI safety evaluator, red-team reviewer, release-gate owner, instructor, and learner	dual-use misuse-risk assessment, safeguard-evidence review, release-gate critique, and frontier-model red-team scope planning with draft-status caveat	safety, misuse prevention, accountability, evaluation validity, incident readiness, and harm reduction	NIST AI 800-1 initial public draft on managing misuse risk for dual-use foundation models; used as draft official guidance, not as finalized regulation.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Group and Panel, 2026]	International AI Safety Report 2026	curriculum_anchor	assurance_evaluation	official_primary	2026-06-12	annual	assurance evaluator, policy reviewer, instructor, system steward, and learner	advanced-AI safety evidence review, uncertainty register, capability-risk synthesis, and policy-neutral assurance briefing	safety, accountability, transparency, uncertainty communication, international coordination, and harm prevention	International AI Safety Report 2026 chaired by Yoshua Bengio with an international expert advisory panel; used as a synthesis source for advanced-AI safety evidence and uncertainty, not as a policy endorsement.
[Project, 2025c]	Specification - Model Context Protocol	curriculum_anchor	agent_interoperability	official_primary	2026-06-11	quarterly	agent-platform engineer, interoperability reviewer, procurement assessor, instructor, and learner	bibliography traceability	interoperability, transparency, least-privilege integration, tool accountability, auditable agent context exchange, and user consent	Official Model Context Protocol specification page for the 2025-06-18 version, grounding agent-tool interoperability language and protocol-boundary examples.
[Project, 2025b]	Security Best Practices - Model Context Protocol	curriculum_anchor	secure_release	official_primary	2026-06-11	quarterly	security architect, release reviewer, agent-platform engineer, instructor, and learner	MCP deployment threat model, confused-deputy mitigation checklist, token-handling review, human-consent gate, least-privilege scope, and release-gate security evidence	security, consent, least privilege, credential protection, accountability, user control, and harm prevention	Official MCP security best practices page describing security considerations, attack vectors, and implementation practices for MCP deployments.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Project, 2025a]	Agent2Agent (A2A) Protocol	curriculum_anchor	agent_interoperability	official_primary	2026-06-06	quarterly	multi-agent system architect, interoperability reviewer, instructor, procurement assessor, and learner	bibliography traceability	interoperability, security, transparency, accountability, and auditable multi-agent coordination	Official Agent2Agent (A2A) protocol documentation describing an open standard for AI agents to securely communicate, collaborate, and coordinate work.
[Centre and international partners, 2024]	Guidelines for Secure AI System Development	curriculum_anchor	secure_release	official_primary	2026-06-06	annual	secure-AI engineer, release reviewer, procurement assessor, instructor, and learner	secure-AI lifecycle review, provider-customer responsibility map, supply-chain checklist, and release-readiness evidence	security, resilience, accountability, supply-chain integrity, transparency, and harm prevention	NCSC Guidelines for secure AI system development for providers of systems that use AI, including systems built from scratch and systems built on top of third-party tools or services.
[MITRE, 2026d]	D3FEND Matrix	curriculum_anchor	assurance_evaluation	official_primary	2026-06-06	quarterly	cyber defense analyst, control assessor, red-team debriefer, instructor, and learner	defensive-control crosswalk, countermeasure-evidence checklist, ATT&CK-to-D3FEND debrief, and assurance remediation backlog	security, defensive proportionality, accountability, resilience, and harm prevention	MITRE D3FEND knowledge base of cybersecurity countermeasure techniques and relationships to offensive/adversary techniques; used to ground defensive-control mapping without operationalizing attacks.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Open, 2022]	Common Security Advisory Framework Version 2.0	curriculum_anchor	records_retention_and_audit_trail	technical_standard	2026-06-12	annual	PSIRT lead, vulnerability coordinator, procurement reviewer, instructor, and learner	security-advisory evidence package, vulnerability-status table, remediation-record review, and supplier disclosure audit	security transparency, accountable disclosure, remediation traceability, procurement accountability, and harm reduction	OASIS Common Security Advisory Framework Version 2.0 standard for machine-readable vulnerability and remediation advisories, used to ground audit-ready incident and procurement evidence.
[Project, 2026a]	CycloneDX Specification Overview	curriculum_anchor	model_data_provenance	technical_standard	2026-06-06	quarterly	supply-chain analyst, SBOM steward, procurement assessor, secure-release reviewer, instructor, and learner	component-inventory evidence, dependency-risk review, supplier BOM checklist, and release-gate provenance record	transparency, supply-chain accountability, security, auditability, and user harm reduction	CycloneDX specification overview for bill-of-materials formats, used to ground component inventory, dependency provenance, and supplier evidence in agentic AI systems.
[SPDX Project, 2024]	SPDX Specification 3.0.1	curriculum_anchor	model_data_provenance	technical_standard	2026-06-06	annual	documentation steward, provenance reviewer, license/compliance assessor, instructor, and learner	SBOM/provenance field checklist, documentation-card evidence, licensing/security review, and audit-trail crosswalk	transparency, accountability, licensing clarity, security, and auditability	SPDX 3.0.1 specification for creating software bills of materials and related machine-readable provenance records; used to ground model/data/software documentation evidence.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of Standards and Technology, 2026j]	OSCAL - Open Security Controls Assessment Language	curriculum_anchor	records_retention	official_publication	2026-06-06	quarterly	control assessor, compliance engineer, audit-trail steward, instructor, and learner	machine-readable control-evidence package, assessment-result review, audit-trail crosswalk, and compliance automation readiness check	accountability, auditability, transparency, security, privacy, and due-process traceability	NIST Open Security Controls Assessment Language project, used to ground machine-readable control catalogs, assessment evidence, and compliance traceability.
[chain Levels for Software Artifacts Project, 2026]	SLSA Specification	curriculum_anchor	software_release_security_standard	standard	2026-06-06	quarterly	release engineer, supply-chain reviewer, procurement assessor, instructor, and learner	release-gate provenance checklist, build-integrity assessment, supply-chain risk review, and rollback evidence package	security, accountability, resilience, transparency, and harm reduction	SLSA specification for describing and incrementally improving software supply-chain security, used to ground artifact provenance and release-control claims.
[in-toto Project, 2026]	in-toto	curriculum_anchor	software_release_security_standard	standard	2026-06-06	quarterly	release engineer, provenance reviewer, assurance evaluator, instructor, and learner	attestation-chain review, provenance evidence package, release-step integrity check, and supplier handoff audit	security, provenance, accountability, auditability, and user protection	in-toto framework for securing software supply-chain integrity with verifiable metadata and attestations; used to ground release-chain evidence and provenance checks.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Project, 2026c]	Overview - Sigstore	curriculum_anchor	software_release_security	standard	2026-06-06	quarterly	release signer, supply-chain security reviewer, procurement assessor, instructor, and learner	artifact-signing evidence, transparency-log verification, release authenticity check, and supply-chain audit trail	security, transparency, accountability, provenance, and harm prevention	Sigstore documentation overview for software signing and transparency-log backed artifact verification, used to ground tamper-evident release and provenance evidence.
[Friston, 2010]	The free-energy principle: a unified brain theory?	curriculum_anchor	cognitive_active_inference	scholarly_peer_reviewed	2026-06-08	annual	source guide context	bibliography traceability	source guide context	Karl Friston's flagship review introducing the free-energy principle, showing how a variational free-energy functional provides a tractable upper bound on surprise (negative log model evidence) that the brain minimizes through perception and action.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Friston, 2017]	Active Inference: A Process Theory	curriculum_anchor	cognitive_active_inference	scholarly_preprint	2026-06-08	annual	source guide context	bibliography traceability	source guide context	Formalizes active inference as a process theory in which belief updating proceeds by gradient descent on variational free energy and policies are selected by minimizing expected free energy over a Markov decision process generative model.
[Da Costa, 2020]	Active inference on discrete state-spaces	curriculum_anchor	cognitive_active_inference	scholarly_preprint	2026-06-08	annual	source guide context	bibliography traceability	source guide context	A mathematical synthesis of active inference over discrete (POMDP) state-spaces, consolidating the partially observable Markov decision process model used to specify perception, planning, and action selection in agentic systems.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Parr, 2022]	Active Inference: The Free Energy Principle in Mind, Brain, and Behavior	curriculum_anchor	cognitive_active_inference	scholarly_preprint	2026-06-08	annual	source guide context	bibliography traceability	source guide context	The open-access MIT Press monograph giving the book-length, chapter-organized foundational treatment of active inference, from the free-energy principle to discrete and continuous generative models and their behavioral implications.
[Yao, 2023a]	ReAct: Synergizing Reasoning and Acting in Language Models	curriculum_anchor	agentic_ai_governance	scholarly_preprint	2026-06-08	annual	source guide context	bibliography traceability	source guide context	Introduces the interleaved reason-then-act loop in which an LLM alternates verbal reasoning traces with tool/environment actions, grounding the reason-act/tool-use pattern at the core of modern agent design.
[Shinn, 2023]	Reflexion: Language Agents with Verbal Reinforcement Learning	curriculum_anchor	agentic_ai_governance	scholarly_preprint	2026-06-08	annual	source guide context	bibliography traceability	source guide context	Proposes agents that verbally reflect on task feedback and store reflections in episodic memory to improve on later trials, grounding the self-reflection and stop-condition pattern for iterative agents.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Park, 2023]	Generative Agents: Interactive Simulacra of Human Behavior	curriculum_anchor	agentic_ai_governance	scholarly_peer_reviewed	2026-06-08	annual	source guide context	bibliography traceability	source guide context	Demonstrates a multi-agent sandbox of twenty-five LLM agents whose memory-stream, reflection, and planning architecture produces believable emergent social behavior, grounding the memory/planning/m agent-simulation pattern.
[Wei, 2022]	Chain-of-Thought Prompting Elicits Reasoning in Large Language Models	curriculum_anchor	agentic_ai_governance	scholarly_preprint	2026-06-08	annual	source guide context	bibliography traceability	source guide context	Shows that prompting an LLM to emit intermediate reasoning steps markedly improves complex reasoning, establishing the reasoning-decomposition pattern that underlies agent planning and ReAct-style traces.
[Schick, 2023]	Toolformer: Language Models Can Teach Themselves to Use Tools	curriculum_anchor	agentic_ai_governance	scholarly_preprint	2026-06-08	annual	source guide context	bibliography traceability	source guide context	Shows an LLM self-supervising when and how to call external APIs (calculator, search, QA, translation, calendar), grounding the tool-use / API-calling pattern for agents.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Wooldridge, 1995]	Intelligent agents: theory and practice	curriculum_anchor	agentic_ai_governance	scholarly_peer_reviewed	2026-06-08	annual	source guide context	bibliography traceability	source guide context	Foundational survey dividing agent research into theory, architectures, and languages, providing the canonical agent definition and multi-agent-systems vocabulary that predates the LLM era.
[Wooldridge, 2009]	An Introduction to MultiAgent Systems, 2nd Edition	curriculum_anchor	agentic_ai_governance	scholarly_textbook	2026-06-08	annual	source guide context	bibliography traceability	source guide context	Standard graduate textbook on multi-agent systems covering coordination, negotiation, voting, and auctions, grounding the multi-agent-coordination vocabulary used in agentic governance.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Burkett, 2013]	An Alternative Framework for Agent Recruitment: From MICE to RASCLS	curriculum_anchor	counterintelligence	official_publication	2026-05-08	annual	source guide context	bibliography traceability	source guide context	A CIA Studies in Intelligence analyst essay arguing that the traditional MICE recruitment-motivation model (Money, Ideology, Compromise, Ego) is better understood through Cialdini's influence principles reframed as RASCLS (Reciprocation, Authority, Scarcity, Commitment/Consistency, Liking, Social Proof), grounding the historical and conceptual lineage of HUMINT recruitment frameworks.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Meissner, 2017]	Developing an Evidence-Based Perspective on Interrogation: A Review of the U.S. Government's High-Value Detainee Interrogation Group Research Program	curriculum_anchor	counterintelligence	scholarly_source	2026-05-08	annual	source guide context	bibliography traceability	source guide context	A peer-reviewed synthesis of the HIG-funded research program summarizing scores of empirical studies showing that rapport-based, non-coercive interviewing reliably outperforms accusatorial or coercive methods for eliciting accurate information, establishing the evidence base for rights-respecting elicitation.
[Brimbal, 2020]	Developing Rapport and Trust in the Interrogative Context: An Empirically Supported Alternative	curriculum_anchor	counterintelligence	scholarly_source	2026-05-08	annual	source guide context	bibliography traceability	source guide context	An Oxford volume chapter reviewing the empirical and ethical case for rapport- and trust-based interrogation as an alternative to customary coercive practices, grounding the contrast between rapport-based and coercive elicitation and the ethics/consent governance that distinguishes them.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Nunan, 2020]	Eliciting human intelligence: police source handlers' perceptions and experiences of rapport during covert human intelligence sources (CHIS) interactions	curriculum_anchor	counterintelligence	scholarly_peer_reviewed	2026-08	annual	source guide context	bibliography traceability	source guide context	A peer-reviewed study of UK police source handlers' lived perceptions of rapport during interactions with covert human intelligence sources, grounding how rapport functions in real source-handler tradecraft and the governance of HUMINT/CHIS relationships.
[Kelly, 2013]	A Taxonomy of Interrogation Methods	curriculum_anchor	counterintelligence	scholarly_peer_reviewed	2026-08	annual	source guide context	bibliography traceability	source guide context	A peer-reviewed taxonomy organizing interrogation into macro-level approaches, six meso-level domains (rapport/relationship building, context manipulation, emotion provocation, confrontation/competition, collaboration, presentation of evidence), and micro-level techniques, providing a study-grounded vocabulary for analyzing elicitation methods rather than an operational manual.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Pherson, 2014a]	Structured Analytic Techniques for Intelligence Analysis	curriculum_anchor	analytic_tradecraft	scholarly_textbook	2026-06-08	annual	source guide context	bibliography traceability	source guide context	The standard practitioner catalogue of fifty-five structured analytic techniques (e.g., Analysis of Competing Hypotheses, Key Assumptions Check, Devil's Advocacy) used to counter cognitive bias in intelligence analysis.
[of Standards and , NIST]	FIPS 197: Advanced Encryption Standard (AES)	curriculum_anchor	cyber_threat_intelligence	standard	2026-06-08	annual	source guide context	bibliography traceability	source guide context	The U.S. federal standard specifying the AES block cipher, the canonical symmetric algorithm providing data confidentiality.
[of Standards and , NIST]	FIPS 186-5: Digital Signature Standard (DSS)	curriculum_anchor	cyber_threat_intelligence	standard	2026-06-08	annual	source guide context	bibliography traceability	source guide context	The U.S. federal standard specifying approved digital-signature algorithms (e.g., ECDSA, EdDSA, RSA) used to authenticate signatories and detect unauthorized data modification.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of Standards and , NIST]	FIPS 180-4: Secure Hash Standard (SHS)	curriculum_anchor	cyber_threat_technical	technical_standard	2026-06-08	annual	source guide context	bibliography traceability	source guide context	The U.S. federal standard specifying the SHA family of cryptographic hash functions used to produce fixed-length digests for data-integrity verification.
[, NIST]	NIST SP 800-57 Part 1 Rev. 5: Recommendation for Key Management, Part 1: General	curriculum_anchor	cyber_threat_technical	technical_standard	2026-06-08	annual	source guide context	bibliography traceability	source guide context	NIST's general guidance on cryptographic key management, covering key types, cryptoperiods, and lifecycle governance across the full key life.
[McGuire, 1961]	Resistance to persuasion conferred by active and passive prior refutation of the same and alternative counterarguments	curriculum_anchor	cognitive_influence	scholarly_secondary	2026-06-08	annual	source guide context	bibliography traceability	source guide context	The founding inoculation-theory experiment, showing that pre-exposing people to weakened counterarguments (refutational pre-bunking) builds resistance to later persuasion better than passive supportive defenses — the medical-vaccination analogy that grounds modern prebunking research.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Mahima Pushkarna and Kjartansson, 2022]	Data Cards: Purposeful and Transparent Dataset Documentation for Responsible AI	curriculum_anchor	dataset_documentation	scholarly_peer_reviewed	2026-06-09	annual	data steward, dataset creator, model owner, assurance reviewer, instructor, learner, and affected-user representative	dataset card review, stakeholder-specific documentation checklist, dataset lifecycle governance, and model/data release evidence	dataset transparency, stakeholder comprehension, fairness review, accountable reuse, and lifecycle documentation	ACM FAccT paper introducing Data Cards as structured, purposeful, human-centered summaries of dataset facts needed by stakeholders across a dataset lifecycle for responsible AI development.
[Christopher L. Buckley and Seth, 2017]	The Free Energy Principle for Action and Perception: A Mathematical Review	curriculum_anchor	cognitive_active_inference	scholarly_preprint	2026-06-10	annual	instructor, learner, assurance reviewer, curriculum maintainer, and governance reviewer	active-inference theory review, classroom analogy boundary setting, formal-claim caveat review, and governance handoff evidence	prevents theory-to-governance overclaiming, separates formal theory from pedagogical analogy, and blocks unsupported autonomous-action claims	arXiv scholarly review that works through the free energy principle and active inference mathematically, including an agent-based model and the assumptions needed for the formal result.
[Melissa L. Rethlefsen and the PRISMA-S Group, 2021]	PRISMA-S: An Extension to the PRISMA Statement for Reporting Literature Searches in Systematic Reviews	curriculum_anchor	source_construction	scholarly_report	2026-06-10	annual	curriculum maintainer, assurance reviewer, instructor, learner, and source-refresh reviewer	source-construction reporting protocol, search-surface documentation, inclusion and exclusion evidence, deduplication notes, and refreshable citation workflow	supports transparent source selection, reproducible search records, auditability, and limits on unverified discovery-source reuse	Systematic Reviews article introducing the PRISMA-S extension, a 16-item checklist for transparent, reproducible reporting of search methods in evidence syntheses.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Kai Greshake and Fritz, 2023]	Not What You've Signed Up For: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection	curriculum_anchor	agentic_ai_security	scholarly_preprint	2026-06-10	annual	agent builder, security reviewer, assurance reviewer, instructor, learner, and incident responder	agentic retrieval and tool-use security review, indirect prompt-injection threat modeling, blocked-action logging, memory-contamination checks, and human escalation evidence	protects users and affected parties from hidden instruction/data blending, unauthorized disclosure, unsafe tool invocation, and contaminated downstream reuse	arXiv security paper showing that malicious third-party content retrieved by LLM-integrated applications can indirectly inject instructions and compromise real-world application behavior.
[of Standards and Technology, 2026b]	Practices for Automated Benchmark Evaluations of Language Models and AI Agent Systems, NIST AI 800-2 Initial Public Draft	curriculum_anchor	assurance_evaluation	official_draft	2026-06-11	quarterly	AI evaluator, procurement assessor, assurance reviewer, instructor, system steward, and learner	automated benchmark evaluation protocol, agent benchmark documentation, validity and reproducibility review, and evaluation-report caveats	validity, reliability, reproducibility, transparency, accountability, procurement review, and documented evaluation limits	NIST AI 800-2 initial public draft provides voluntary practices for automated benchmark evaluations of language models and AI agent systems.
[for Economic Co-operation and Development, 2026a]	The Agentic AI Landscape and Its Conceptual Foundations	curriculum_anchor	agent_interoperability	official_publication	2026-06-11	semiannual	policy analyst, standards steward, curriculum maintainer, instructor, and learner	agentic AI definition crosswalk, standards landscape map, policy-neutral concept boundary, and adoption-trend caveat review	conceptual clarity, public-policy coherence, transparent terminology, accountability, and bounded claims about agentic capability	OECD AI paper clarifying the agentic AI landscape and conceptual foundations by comparing definitions and mapping shared features to the OECD AI system definition.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Agency, 2026i]	Model Context Protocol (MCP): Security Design Considerations for Organizations	curriculum_anchor	secure_release_gate	official_primary	2026-06-11	quarterly	security architect, release reviewer, agent-platform engineer, procurement assessor, instructor, and learner	MCP security design review, implementation threat model, privilege boundary checklist, reverse-proxy and sandboxing control discussion, and secure-release gate evidence	security, credential protection, least privilege, supply-chain integrity, sandboxing, auditability, and harm prevention	NSA cybersecurity information sheet on MCP security design considerations for organizations adopting MCP-based AI toolchains.
[Jon Roozenbeek and Lewandowsky, 2022]	Psychological Inoculation Improves Resilience Against Misinformation on Social Media	curriculum_anchor	cognitive_resilience	scholarly_peer_reviewed	2026-06-11	annual	instructor, cognitive-security reviewer, learner, assurance reviewer, and affected-community representative	prebunking evidence boundary, inoculation mechanism caveat, outcome-measure review, and cognitive-security lesson-scope limits	cognitive autonomy, transparent educational framing, anti-manipulation safeguards, measured-outcome limits, and rights-aware prebunking practice	Science Advances article showing that psychological inoculation campaigns on social media can improve misinformation resilience at scale under measured study conditions.
[for the Study of Intelligence, 2002]	Sherman Kent and the Profession of Intelligence Analysis	curriculum_anchor	analytic_tradecraft	official_primary	2026-06-11	annual	curriculum designer; analytic tradecraft instructor; analyst supervisor	Grounds professional-standards framing for tradecraft lessons.	public-domain government source; cite as historical context	Official CIA Center for the Study of Intelligence essay on Kent's professionalization of intelligence analysis and analytic standards.
[for the Study of Intelligence, 1994]	Sherman Kent's Final Thoughts on Analyst-Policymaker Relations	curriculum_anchor	analytic_tradecraft	official_primary	2026-06-11	annual	analytic tradecraft instructor; policy liaison; analyst supervisor	Keeps warning and policy-support lessons inside advisory rather than decision-authority claims.	public-domain government source; cite as historical context	Official CIA CSI republication of Kent's final essay on analyst-policy relations, warning, intention, and communication boundaries.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Wohlstetter, 1962]	Pearl Harbor: Warning and Decision	curriculum_author	warning_intelligence	high_scholarly_publication_record	2026-06-11	annual	curriculum designer; intelligence history instructor	Frames warning lessons around indicators, noise, and uncertainty rather than hindsight certainty.	copyrighted scholarly book metadata only; do not reproduce extended text	Publisher record for Wohlstetter's classic warning-intelligence study of signal, noise, and surprise before Pearl Harbor.
[Grabo, 1972]	Handbook of Warning Intelligence	curriculum_author	warning_intelligence	official_declassified_primary	2026-06-11	annual	analytic tradecraft instructor; warning-methods reviewer	Adds source-backed warning vocabulary while preserving evidence-bounded educational boundaries.	declassified public government record; avoid operationalizing historical procedures	CIA Reading Room declassified warning-intelligence handbook volume used for indications-and-warning concepts.
[Congress, 2004]	Intelligence Reform and Terrorism Prevention Act of 2004	curriculum_author	intelligence_failure	official_post_mortem	2026-06-11	biennial	curriculum designer; governance reviewer; public-sector analyst	Links tradecraft standards to public-law reform context without turning law into technique guidance.	public-domain legal source; preserve statutory context	Official GovInfo public law record establishing post-9/11 intelligence reform requirements including alternative analysis and analytic integrity provisions.
[on Terrorist Attacks Upon the United States, 2004]	The 9/11 Commission Report	curriculum_author	intelligence_failure	official_post_mortem_report	2026-06-11	biennial	curriculum designer; governance reviewer; analyst supervisor	Connects warning lessons to post-mortem learning and reform without hindsight simplification.	public-domain government report; cite official source	Official commission report used for post-mortem context on warning, information sharing, imagination, and reform pressures after September 11, 2001.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005]	Report to the President of the United States: The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction	curriculum_and_training	intelligence_failure_and_reform	official_publication	2026-06-11	biennial	curriculum designer; governance reviewer; analytic tradecraft instructor	Shows why evidence boundaries, dissent, and assumption registers matter in high-consequence analysis.	public-domain government report; cite official source	Official WMD Commission report used for Iraq WMD analytic-failure context, assumptions-versus-evidence boundaries, and reform pressure.
[Transformation, 2017]	Alternative Analysis Handbook	curriculum_and_training	analytic_tradecraft	official_publication	2026-06-11	annual	analytic tradecraft instructor; team facilitator; curriculum designer	Provides official practice examples for alternative-analysis workflows.	official alliance publication; cite handbook and avoid long excerpts	Official NATO handbook presenting alternative-analysis techniques and facilitation practices for analytic teams.
[Bruce, 2016]	Assessing the Value of Structured Analytic Techniques in the U.S. Intelligence Community	curriculum_and_training	research_and_evaluation	policy_research	2026-06-15	annual	curriculum designer; evaluation lead; analyst supervisor	Prevents overclaiming that SATs generally cure bias or guarantee accuracy.	RAND copyrighted report; cite metadata and summarize sparingly	RAND report on the difficulty of measuring SAT value and the need for systematic evaluation before strong effectiveness claims.
[Alexandru Marcoci and Jonas, 2019]	Better Together: Reliable Application of the Post-9/11 and Post-Iraq US Intelligence Tradecraft Standards Requires Collective Analysis	curriculum_and_training	research_and_evaluation	scholarly_evidence	2026-06-11	annual	curriculum designer; quality reviewer; analytic standards trainer	Grounds reviewer calibration, aggregate judgment, and quality-control lessons.	open-access scholarly article; cite DOI/journal source	Peer-reviewed study showing poor individual reliability but stronger aggregated reliability when raters apply tradecraft standards to intelligence reports.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Barnes and Mandel, 2014]	Accuracy of Forecasts in Strategic Intelligence	curriculum_anchor	forecasting_calibration	scholarly_peer_reviewed	2026-06-11	annual	curriculum designer; forecasting instructor; evaluation lead	Links probability language and calibration exercises to empirical forecasting evidence.	copyrighted scholarly article; cite metadata and avoid extended quotation	Peer-reviewed PNAS study of strategic-intelligence forecast accuracy, calibration, discrimination, and probability-language behavior.
[Ard, 2024]	Structured Analytic Techniques: A Pragmatic Approach	curriculum_anchor	evaluation_scholarship	scholarly_peer_reviewed	2026-06-15	annual	curriculum designer; analytic standards trainer; evaluation lead	Forces SAT lessons to distinguish transparency aids from demonstrated accuracy improvements.	copyrighted scholarly article; cite DOI metadata and summarize sparingly	Peer-reviewed critique arguing that SAT evidence is thinner than many tradecraft claims imply and that SATs should not be treated as universal bias remedies.
[Jennifer Stromer-Galley and colleagues, 2020]	Flexible Versus Structured Support for Reasoning: Enhancing Analytical Reasoning Through a Flexible Analytic Technique	curriculum_anchor	evaluation_scholarship	repository_record	2026-06-11	annual	curriculum designer; analytic standards trainer; evaluation lead	Adds a positive but bounded empirical counterpoint to SAT critique and doctrine sources.	repository metadata and scholarly article; cite source and avoid extended quotation	Scholarly record and abstract for an experimental comparison of flexible SAT support and structured/no-SAT conditions for reasoning quality.
[Betts, 1978]	Analysis, War, and Decision: Why Intelligence Failures Are Inevitable	curriculum_anchor	intelligence_failure	scholarly_postpeer_review	2026-06-11	annual	curriculum designer; intelligence history instructor; governance reviewer	Keeps failure lessons attentive to policy uptake, incentives, and organizational learning.	copyrighted scholarly article metadata; cite and summarize sparingly	Classic peer-reviewed failure-theory article on the interaction of analysis, decision, leadership psychology, and policy uptake.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Jervis, 2022]	Why Intelligence and Policymakers Clash	curriculum_architect	intelligence_failure	scholarly_postmortem	2026-06-11	annual	curriculum designer; governance reviewer; analyst supervisor	Constrains post-mortem lessons so they do not imply a single technique could prevent complex failure.	copyrighted scholarly article; cite metadata and summarize sparingly	PNAS perspective on intelligence-policy friction and the limits of post-mortem explanations of intelligence failure.
[Wirtz, 2023]	Are Intelligence Failures Still Inevitable?	curriculum_architect	intelligence_failure	scholarly_postmortem	2026-06-11	annual	curriculum designer; governance reviewer; analytic standards trainer	Links classic failure theory to contemporary reform and warning lessons.	copyrighted scholarly article; cite DOI metadata and summarize sparingly	Peer-reviewed discussion revisiting intelligence-failure inevitability in light of collection, analysis, reform, and policy factors.
[Central Intelligence Agency, 1993]	Words of Estimative Probability	curriculum_architect	analytic_uncertainty	official_primary	2026-06-14	annual	analyst, reviewer, method instructor	checks whether probability words, confidence, and evidence limits remain separated	public professional literature used for education and review without operational tasking	CIA/CSI source for disciplined probability language and the review boundary between estimative wording, evidence, and numeric interpretation.
[Central Intelligence Agency, 1970s]	The IC's Struggle to Express Uncertainty in the 1970s	curriculum_architect	analytic_uncertainty	official_primary	2026-06-14	annual	analyst, reviewer, writing coach	anchors exercises that separate likelihood, confidence, dissent, and caveats	public professional literature used for education and review without operational tasking	CIA/CSI historical source for uncertainty vocabulary, disagreement, and estimative communication problems.
[Central Intelligence Agency, 2018b]	Developing a Taxonomy of Intelligence Analysis Variables	curriculum_architect	analytic_methods	official_primary	2026-06-14	annual	method designer, reviewer, instructor	supports modular decomposition of claims, variables, evidence, and uncertainty	public professional literature used for education and review without operational tasking	CIA/CSI analytic-methods source for decomposing analysis variables and avoiding one-piece judgment claims.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Johnston, 2005]	Analytic Culture in the U.S. Intelligence Community	curriculum_anchor	intelligence_profession	official_publication	2026-06-15	annual	curriculum designer, analyst, reviewer	keeps culture and training claims tied to official professional context rather than slogans	public professional literature used for education and review without operational tasking	CIA/CSI professional-literature monograph on analytic institutions, incentives, training, and cultural constraints.
[Central Intelligence Agency, 1955]	The Need for an Intelligence Literature	curriculum_anchor	intelligence_profession	official_publication	2026-06-14	annual	method instructor, author, reviewer	anchors claims that AGEINT is an inspectable literature-backed substrate, not a private prompt collection	public professional literature used for education and review without operational tasking	Classic CIA/CSI source for why intelligence practice needs a professional literature and reviewable doctrine.
[Central Intelligence Agency, 2025b]	Studies in Intelligence Author's Guide 2025: Guidance Section Only	curriculum_anchor	intelligence_writing	official_publication	2026-06-14	annual	author, editor, reviewer	supports writing gates that distinguish public professional analysis from agency policy or operational direction	public professional guidance used for education and manuscript review	CIA/CSI writing-guide source for public professional writing norms, review boundaries, and publication discipline.
[Central Intelligence Agency, 2025a]	Applying Epistemology to Intelligence Analysis	curriculum_anchor	analytic_epistemology	official_publication	2026-06-14	annual	analyst, epistemic reviewer, instructor	supports claim-calibration language about what evidence can and cannot establish	public professional literature used for education and review without operational tasking	CIA/CSI source for epistemic framing, objectivity, knowledge claims, and analytic habits of thinking.
[Central Intelligence Agency, 2023]	Agile Analysis: Transforming Intelligence Production Through Lean Startup Principles	curriculum_anchor	analytic_production	official_publication	2026-06-14	annual	team lead, analyst, reviewer	anchors modular workflow claims while preserving human review and experiment limits	public professional literature used for education and review without operational tasking	CIA/CSI source for team-based analytic production, iteration, and experimentation boundaries.
[Central Intelligence Agency, 2018c]	Managing the Reliability Cycle: An Alternative Approach to Thinking About Intelligence Failure	curriculum_anchor	intelligence_failure	official_publication	2026-06-14	annual	reviewer, red team, instructor	supports negative-control and after-action learning language	public professional literature used for education and review without operational tasking	CIA/CSI source for reliability, intelligence failure, feedback, and institutional learning cycles.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Central Intelligence Agency, 2018f]	Why Bad Things Happen to Good Analysts	curriculum_anchor	intelligence_failure	official_publication	2026-06-14	annual	analyst, reviewer, instructor	supports lessons that distinguish reviewable practice from proof of correctness	public professional literature used for education and review without operational tasking	CIA/CSI source for analyst error, limits, and institutional conditions around analytic failure.
[Central Intelligence Agency, 2019]	The Future of Analysis	curriculum_anchor	ai_enabled_analysis	official_publication	2026-06-14	annual	analyst, AI governance reviewer, instructor	anchors agentic-assistance claims to professional context and limits	public professional literature used for education and review without operational tasking	CIA/CSI source for future analytic work, data volume, automation, and human analytic structure.
[Central Intelligence Agency, 1999]	Psychology of Intelligence Analysis	curriculum_anchor	analytic_cognition	official_publication	2026-06-14	annual	analyst, instructor, reviewer	supports misconception checks and cognitive-bias caveats in topic lessons	public professional literature used for education and review without operational tasking	CIA/CSI public PDF of Richards Heuer's work on cognition, bias, evidence evaluation, and analytic judgment.
[Central Intelligence Agency, 1994]	Sherman Kent and the Board of National Estimates: Collected Essays	curriculum_anchor	declassified_analytic_history	official_publication	2026-06-14	annual	historian, analyst, reviewer	keeps historical institutional claims tied to declassified official material	public declassified history used for education and governance lessons	CIA/CSI historical professional source for estimative practice, institutional review, and the Board of National Estimates.
[Central Intelligence Agency, 2020]	Lessons from SABLE SPEAR: The Application of an Artificial Intelligence Methodology to Tactical Intelligence	curriculum_anchor	ai_enabled_analysis	official_publication	2026-06-14	annual	AI governance reviewer, analyst, instructor	supports examples that keep AI assistance reviewable, bounded, and evidence-bounded	public professional literature used for education and review without operational tasking	CIA/CSI article on an AI-enabled analytic experiment, used as bounded professional context for AI-assisted analysis.
[Central Intelligence Agency, 2018a]	A Call for More Humility in Intelligence Analysis	curriculum_anchor	analytic_cognition	official_publication	2026-06-14	annual	analyst, reviewer, instructor	anchors reviewer checklists that ask what evidence does not establish	public professional literature used for education and review without operational tasking	CIA/CSI article supporting humility, uncertainty, and limits in analytic judgment.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Central Intelligence Agency, 2021a]	Voice of Experience: Principles of Intelligence Analysis	curriculum_anchor	analytic_method	official_publication	primary	2026-06-14	annual	analyst, instructor, reviewer	supports modular practice-language around evidence, assumptions, and judgment	public professional literature used for education and review without operational tasking	CIA/CSI article on foundational elements of intelligence analysis and disciplined analytic practice.
[Central Intelligence Agency, 2018e]	War and Chance: Assessing Uncertainty in International Politics	curriculum_anchor	analytic_uncertainty	official_publication	primary	2026-06-14	annual	analyst, instructor, reviewer	supports wording that avoids proof, certainty, or overconfident statistical implication	public professional literature used for education and review without operational tasking	CIA/CSI review source for uncertainty, probability expression, and the limits of confident prediction.
[Central Intelligence Agency, 2005a]	Fifty Years of Studies in Intelligence	curriculum_anchor	intelligence_profession	official_publication	primary	2026-06-14	annual	author, reviewer, historian	supports claims about public professional literature as a reviewable source surface	public professional literature used for education and review without operational tasking	CIA/CSI reflection on Studies in Intelligence as an official professional literature venue.
[Central Intelligence Agency, 2018d]	Thinking and Writing: Cognitive Science and Intelligence Analysis	curriculum_anchor	intelligence_writing	official_publication	primary	2026-06-14	annual	author, analyst, reviewer	supports prose gates that demand concrete claims, caveats, and reader-inspectable reasoning	public professional literature used for education and review without operational tasking	CIA/CSI source connecting cognitive science, analytic writing, and intelligence-analysis communication.
[Central Intelligence Agency, 2005b]	Creation of a National Institute for Analytic Methods	curriculum_anchor	analytic_method	official_publication	primary	2026-06-14	annual	method designer, evaluator, reviewer	anchors method claims to reviewable institutional evaluation needs rather than intuition	public professional literature used for education and review without operational tasking	CIA/CSI source on analytic-method evaluation, evidence standards, and institutional method development.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Central Intelligence Agency, 2006]	When Everything is Intelligence - Nothing is Intelligence	curriculum_anchor	intelligence_foundations	official_primary	2026-06-14	annual	analyst, instructor, reviewer	helps prevent source availability from being treated as analytic judgment	public professional literature used for education and review without operational tasking	CIA/CSI article for defining intelligence analysis around uncertainty rather than undifferentiated information processing.
[Central Intelligence Agency, 1998]	CIA and the Vietnam Policymakers: Three Episodes 1962-1968	curriculum_anchor	declassified_analytic_history	official_primary	2026-06-14	annual	historian, analyst, policy reviewer	anchors historical case discussion without translating it into current operational procedure	public declassified history used for education and governance lessons	CIA/CSI declassified historical source for analyst-policy boundary lessons and historical interpretation limits.
[Central Intelligence Agency, 2021b]	Intelligent Analysis: How to Defeat Uncertainty in High-Stakes Decisions	curriculum_anchor	analytic_uncertainty	official_primary	2026-06-14	annual	analyst, reviewer, instructor	supports calibrated uncertainty language without implying AGEINT benchmark results	public professional literature used for education and review without operational tasking	CIA/CSI review source for uncertainty-management literature and analytic decision support.
[Central Intelligence Agency, 2017]	The Limits of Prediction - or, How I Learned to Stop Worrying About Black Swans and Love Analysis	curriculum_anchor	forecasting_calibration	official_primary	2026-06-14	annual	analyst, forecaster, reviewer	anchors rejection of overstrong prediction, proof, and benchmark claims	public professional literature used for education and review without operational tasking	CIA/CSI source for prediction limits, forecasting caution, and analytic improvement boundaries.
[Central Intelligence Agency, 2026]	Espionage in Our AI Future	curriculum_anchor	ai_enabled_analysis	official_primary	2026-06-14	annual	AI governance reviewer, analyst, counterintelligence instructor	supports safe framing of AI assistance, espionage risk, and reviewer control without operational instructions	public professional literature used for education and review without operational tasking	CIA/CSI 2026 article for AI-era espionage context, source skepticism, and human-review boundaries.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of the Director of National Intelligence, 2026a]	Annual Threat Assessment of the U.S. Intelligence Community 2026	curriculum_anchor	current_threat_baseline	official_publication	primary	2026-06-14	annual	analyst, instructor, policy reviewer	anchors public threat-context examples to an official unclassified IC baseline	public unclassified report used for education and contextual analysis	ODNI unclassified annual threat assessment used as current public threat-context baseline, not as operational guidance.
[of the Director of National Intelligence, 2013a]	Intelligence Community Directive 205: Analytic Outreach	curriculum_anchor	analytic_outreach	official_governance	primary	2026-06-14	annual	analyst, outreach lead, reviewer	supports source-pack routing for external expertise while preserving CI, privacy, and citation boundaries	public directive used for governance education, not outreach tasking	ODNI directive for analytic outreach, outside expertise, risk management, and citation of outreach insights.
[of the Director of National Intelligence, 2008]	Intelligence Community Directive 207: National Intelligence Council	curriculum_anchor	national_intelligence	official_governance	primary	2026-06-14	annual	analyst, instructor, governance reviewer	anchors national intelligence council references to public ODNI policy text	public directive used for governance education and source routing	ODNI directive describing the National Intelligence Council and national intelligence production responsibilities.
[of the Director of National Intelligence, 2017b]	Intelligence Community Directive 208: Maximizing the Utility of Analytic Products	curriculum_anchor	analytic_product	official_dissemination	primary	2026-06-14	annual	analyst, editor, dissemination reviewer	supports generated prose about product utility, reusable evidence packets, and customer-aware outputs	public directive used for governance education, not release authorization	ODNI directive for customer utility, analytic standards, tearlines, discoverability, and transparent products.
[of the Director of National Intelligence, 2012]	Intelligence Community Directive 209: Tearline Production and Dissemination	curriculum_anchor	tearlines_and_dissemination	official_governance	primary	2026-06-14	annual	analyst, disclosure reviewer, instructor	anchors safe discussion of sanitized outputs without teaching live release decisions	public directive used for governance education, not disclosure authorization	ODNI directive for tearlines and broader dissemination while protecting sources and methods.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of the Director of National Intelligence, 2013b]	Intelligence Community Directive 403: Foreign Disclosure and Release of Classified National Intelligence	curriculum_anchor	foreign_disclosure	official_governance	primary	2026-06-14	annual	disclosure reviewer, analyst, instructor	supports evidence-bounded disclosure-boundary teaching and release-control caveats	public directive used for governance education, not disclosure authorization	ODNI directive for foreign disclosure and release governance, marking, records, and release authority.
[of the Director of National Intelligence, 2024a]	Intelligence Community Directive 405: Intelligence Diplomacy	curriculum_anchor	intelligence_diplomacy	official_governance	primary	2026-06-14	annual	policy reviewer, analyst, instructor	keeps diplomacy references policy-bound and evidence-bounded	public directive used for governance education, not diplomatic action guidance	ODNI directive for intelligence diplomacy, synchronization, and foreign-policy support boundaries.
[of the Director of National Intelligence, 2024b]	Intelligence Community Directive 406: IC Engagement with Non-State Entities	curriculum_anchor	state_engagement	official_governance	primary	2026-06-14	annual	outreach lead, analyst, reviewer	anchors public-source and expert-engagement rules without authorizing collection tasking	public directive used for governance education and civil-liberties framing	ODNI directive for non-state entity engagement, analytic outreach, privacy/civil-liberties, and no-tasking boundaries.
[of the Director of National Intelligence, 2024c]	Intelligence Community Directive 503: Intelligence Community Information Environment Risk Management	curriculum_anchor	information_environment	official_governance	primary	2026-06-14	annual	security reviewer, system owner, instructor	supports modular substrate controls around access, risk, and auditability	public directive used for governance education, not classified-system design	ODNI directive for risk management in the IC information environment.
[of the Director of National Intelligence, 2013f]	Intelligence Community Directive 900: Integrated Mission Management	curriculum_anchor	integrated_mission	official_governance	primary	2026-06-14	annual	mission manager, analyst, governance reviewer	anchors mission-alignment language in public ODNI policy	public directive used for governance education and source routing	ODNI directive for integrated mission management and IC mission alignment.
[of the Director of National Intelligence, 2017a]	Intelligence Community Directive 121: Managing the Intelligence Community Information Environment	curriculum_anchor	information_environment	official_governance	primary	2026-06-14	annual	system owner, analyst, reviewer	anchors substrate modularity in information-sharing and safeguarding governance	public directive used for governance education, not classified system operation	ODNI directive for the IC information environment, discovery, retrieval, sharing, and safeguarding.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of the Director of National Intelligence, 2022]	Intelligence Community Directive 211: IC Support to the CFIUS Threat Analysis Process	curriculum_anchor	economic_security	official_primary	2026-06-14	annual	economic-security analyst, reviewer, instructor	supports safe CFIUS-context teaching without transaction targeting or proprietary data use	public directive used for governance education and due-diligence framing	ODNI directive for intelligence support to CFIUS threat analysis, economic-security review, and covered transactions.
[of the Director of National Intelligence, 2013d]	Intelligence Community Directive 731: Supply Chain Risk Management	curriculum_anchor	supply_chain_risk	official_primary	2026-06-14	annual	procurement reviewer, security analyst, instructor	supports supplier-risk and source-integrity language without evasion or exploitation guidance	public directive used for governance education and defensive assurance	ODNI directive for IC supply-chain risk management across mission-critical products, materials, and services.
[of the Director of National Intelligence, 2013c]	Intelligence Community Directive 710: Classification and Control Markings System	curriculum_anchor	classification_marking	official_primary	2026-06-14	annual	marking reviewer, analyst, instructor	anchors marking references to public ODNI policy without handling classified material	public directive used for governance education, not classification authority	ODNI directive for classification and control markings, including release and foreign-disclosure marking relationships.
[of the Director of National Intelligence, 2013e]	Intelligence Community Directive 750: Counterintelligence Programs	curriculum_anchor	counterintelligence	official_primary	2026-06-14	annual	CI reviewer, analyst, instructor	supports defensive CI/source-integrity language without surveillance or handling playbooks	public directive used for governance education and defensive source-integrity framing	ODNI directive establishing a baseline for counterintelligence programs across the IC.
[Intelligence.gov, 2026e]	Mission	curriculum_anchor	public_transparency	official_primary	2026-06-14	quarterly	learner, instructor, reviewer	anchors introductory IC mission language to the public official portal	public education page used for orientation and transparency framing	Intelligence.gov public mission page describing the IC mission, customers, and values at a high level.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Intelligence.gov 2026b]	Our Values: Accountability	curriculum_anchor	public_transparency	official_primary	2026-06-14	quarterly	learner, instructor, civil-liberties reviewer	anchors public-facing accountability language and oversight explanations	public education page used for rights, accountability, and oversight framing	Intelligence.gov public values page describing IC accountability, lawfulness, oversight, and civil liberties framing.
[Intelligence.gov 2026f]	Our Values: Transparency	curriculum_anchor	public_transparency	official_primary	2026-06-14	quarterly	learner, instructor, transparency reviewer	supports transparent manuscript and evidence-packet posture without exposing sources or methods	public education page used for transparency and public-trust framing	Intelligence.gov public values page describing transparency principles, public understanding, and protection of sources and methods.
[Intelligence.gov 2026a]	About This Site	curriculum_anchor	public_transparency	official_primary	2026-06-14	quarterly	learner, instructor, publication reviewer	anchors public-facing transparency language used in AGEINT release-surface checks	public education page used for transparency and public-readiness framing	Intelligence.gov public page explaining the site as an IC transparency platform and public front door.
[Intelligence.gov 2026c]	Our Values: Collaboration	curriculum_anchor	public_transparency	official_primary	2026-06-14	quarterly	learner, instructor, reviewer	supports modular substrate language about collaboration without implying live liaison or tasking	public education page used for orientation and governance framing	Intelligence.gov public values page describing collaboration across IC elements and external partners.
[Intelligence.gov 2026d]	Our Values: Innovation	curriculum_anchor	public_transparency	official_primary	2026-06-14	quarterly	learner, instructor, innovation reviewer	keeps innovation claims tied to public IC values rather than unchecked automation	public education page used for orientation and technology-governance framing	Intelligence.gov public values page describing innovation as more than technology and tying it to mission needs.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Agency, 2024b]	Defense OSINT Strategy 2024-2028	curriculum_anchor	defense_osint	official_primary	2026-06-14	annual	OSINT analyst, instructor, reviewer	anchors OSINT modules to official public Defense governance and source-quality discipline	public strategy used for education and lawful-source governance	DIA strategy for professionalizing and unifying Defense OSINT collection and reporting in public governance terms.
[Agency, 2015]	DIA Style Manual for Intelligence Production	curriculum_anchor	intelligence_writing	official_primary	2026-06-14	annual	author, editor, reviewer	supports AGEINT writing conventions and source-backed manuscript-polish gates	public FOIA release used for education and writing review	DIA public FOIA release for intelligence-production style, terminology, formatting, and writing consistency.
[Agency, 2014]	DIA Instruction 5400.001: Privacy and Civil Liberties Program	curriculum_anchor	rights_impact	official_primary	2026-06-14	annual	privacy reviewer, analyst, instructor	anchors rights-impact review language in an official DIA public instruction	public instruction used for privacy and civil-liberties education	DIA public instruction for privacy and civil-liberties responsibilities, complaints, records, and safeguards.
[Agency, 2026f]	NSA Cybersecurity Advisories and Guidance	curriculum_anchor	cyber_defense	official_primary	2026-06-14	quarterly	cyber analyst, instructor, reviewer	supports defensive CTI source routing without citing exploit instructions	public guidance index used for defensive education and source-refresh planning	NSA public index for cybersecurity advisories, information sheets, technical reports, and operational risk notices.
[Agency, 2026d]	About NSA Mission	curriculum_anchor	public_transparency	official_primary	2026-06-14	quarterly	learner, instructor, reviewer	anchors public NSA mission descriptions to the official page	public education page used for orientation and governance framing	NSA public mission page for SIGINT and cybersecurity mission context.
[Agency, 2026e]	NSA Joins the ASD's ACSC and Others to Release Guidance on Agentic Artificial Intelligence Systems	curriculum_anchor	agentic_ai_security	official_primary	2026-06-14	quarterly	AI security reviewer, system owner, instructor	supports agentic AI safety-boundary and adoption-gate language	public cybersecurity release used for defensive AI-governance education	NSA public release announcing joint guidance on careful adoption of agentic AI services.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Agency, 2017b]	GEOINT Basic Doctrine Publication 1	curriculum_anchor	cohort_professional	official_primary	2026-06-14	annual	GEOINT analyst, instructor, reviewer	anchors GEOINT modules to official doctrine rather than broad imagery claims	public doctrine used for education and source-provenance review	NGA doctrine source for GEOINT definitions, mission context, and professional geospatial intelligence framing.
[Agency, 2021]	NGA Releases New Data Strategy to Navigate Digital, GEOINT Revolution	curriculum_anchor	cohort_data_governance	official_primary	2026-06-14	annual	GEOINT data steward, analyst, reviewer	supports data-lineage and GEOINT-source governance language	public release used for education and data-governance framing	NGA public release on data strategy, geospatial data management, and digital transformation in GEOINT.
[of Investigation, 2026]	Counterintelligence and Espionage	curriculum_anchor	cohort_counterintelligence	official_primary	2026-06-14	quarterly	CI reviewer, analyst, instructor	supports defensive CI/source-integrity framing without investigation procedure or surveillance guidance	public education page used for defensive awareness and source-protection framing	FBI public counterintelligence page describing defensive goals and protection of IC secrets, critical assets, and sensitive information.
[Office, 2026b]	About NRO History	curriculum_anchor	declassified_reconnaissance	official_primary	2026-06-14	annual	historian, GEOINT analyst, instructor	anchors national reconnaissance history to official declassified-history resources	public history page used for education and source-provenance review	NRO public history page describing the Center for the Study of National Reconnaissance and declassified history resources.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Dylan and Stivang, 2025]	Emerging Technologies and National Security Intelligence	curriculum_anchor	ai_enabled_analysis	scholarly_preprint	2026-06-15	annual	analyst, AI governance reviewer, instructor, curriculum maintainer	emerging-technology source review, AI-assisted analysis boundary setting, and medium-term tradecraft refresh planning	accountability, public trust, privacy, and reviewable use of emerging technology in intelligence education	Peer-reviewed Intelligence and National Security article on emerging technologies and national security intelligence, used to frame AI and data-system effects as medium-term intelligence-work pressures requiring analytic governance.
[Caballero and Jenkins, 2024]	On Large Language Models in National Security Applications	curriculum_anchor	ai_enabled_analysis	scholarly_preprint	2026-06-15	semiannual	AI governance reviewer, analyst, instructor, red-team reviewer	LLM assistance risk review, human-judgment boundary checks, and national-security classroom case framing	privacy, reliability, human accountability, adversarial robustness, and public trust	arXiv preprint on LLMs in national-security applications, useful for classroom risk framing because it explicitly treats LLMs as support tools needing safeguards rather than strategic decision-makers.
[Mikhailov, 2023]	Optimizing National Security Strategies through LLM-Driven Artificial Intelligence Integration	curriculum_anchor	ai_enabled_analysis	scholarly_preprint	2026-06-15	semiannual	policy analyst, AI governance reviewer, instructor	strategic-AI claim calibration and cautionary national-security AI planning context	human oversight, strategic accountability, institutional due care, and non-escalatory educational framing	arXiv preprint on LLM-driven AI integration in national-security strategy, encoded with a narrow claim scope because it is useful as a strategic-policy framing source rather than as empirical validation.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Revanth Gangi Reddy and Ji, 2023]	SmartBook: AI-Assisted Situation Report Generation for Intelligence Analysts	curriculum_anchor	enabled_analysis	early_prototype	2026-06-15	semiannual	analyst, instructor, AI product reviewer, assurance evaluator	AI-assisted analytic product review, source-grounding checklist design, and classroom situation-report caveats	source traceability, analyst comprehension, transparency, and non-automation of judgment	SmartBook preprint describing AI-assisted situation-report generation for intelligence analysts, including source grounding, analyst preferences, and evaluation caveats relevant to generated-product review.
[et al., 2024a]	Mind the Gap: Foundation Models and the Covert Proliferation of Military Intelligence, Surveillance, Target Acquisition, and Reconnaissance	curriculum_anchor	enabled_analysis	early_prototype	2026-06-15	semiannual	AI safety reviewer, intelligence educator, policy analyst, red-team reviewer	foundation-model risk boundary, ISTAR claim calibration, and covert-proliferation scenario review	non-proliferation, civilian protection, escalation risk, and human accountability	arXiv HTML source on foundation models and covert proliferation of military ISTAR capabilities, routed as a risk-boundary source for synthetic and defensive education.
[et al., 2023a]	The Age of Synthetic Realities: Challenges and Opportunities	curriculum_anchor	synthetic_media_literacy	scholarly_preprint	2026-06-15	semiannual	cognitive-security reviewer, media-literacy instructor, AI governance reviewer	synthetic media provenance review, deepfake risk caveats, and synthetic-reality classroom examples	identity protection, consent, provenance, public trust, and harms from synthetic media	arXiv survey-style source on synthetic realities and AI-generated media risk, used for provenance, detection-limit, and public-trust framing in cognitive-security lessons.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[et al., 2018]	The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation	curriculum_anchor	red_team_scenario_library	secondary_report	2026-06-15	annual	red-team reviewer, AI governance lead, instructor, safety reviewer	AI misuse taxonomy review, red-team scenario boundaries, and safe substitution design	safety, security, public trust, civil liberties, and defensive risk communication	Foundational public report on malicious uses of AI, encoded for defensive taxonomy, safe-substitution, and governance framing in synthetic classroom work.
[for Security and Technology, 2022]	Adversarial Machine Learning and Cybersecurity	curriculum_anchor	red_team_playbook	public_domain_primary	2026-06-15	annual	AI security reviewer, cyber analyst, instructor, red-team reviewer	adversarial-ML threat-model review, defensive cyber-AI control mapping, and AI assurance caveats	system integrity, safety, defensive security, accountability, and public trust	CSET policy-research source on adversarial machine learning and cybersecurity, used to connect AI model robustness, defensive assurance, and cyber threat-intelligence review.
[Taddeo and Floridi, 2018]	Regulate Artificial Intelligence to Avert Cyber Arms Race	curriculum_anchor	cyber_threat_intelligence	secondary_commentary	2026-06-15	annual	policy reviewer, cyber instructor, governance analyst	AI-cyber escalation caveat, policy-risk review, and cyber-arms-race boundary setting	non-escalation, public safety, accountability, proportionality, and international stability	Nature Comment article arguing for AI-cyber governance before escalation risks intensify, useful for high-level cyber policy and non-escalatory classroom framing.
[Project and Institute, 2024]	The Future of Intelligence Analysis: U.S.-Australia Project on AI and Human-Machine Teaming	curriculum_anchor	ai_enabled_analysis	public_domain_primary	2026-06-15	annual	analytic manager, AI governance reviewer, instructor, alliance liaison educator	human-machine teaming review, analytic-workflow modernization caveats, and alliance-interoperability discussion	human oversight, analytic accountability, alliance coordination, lawful use, and public trust	SCSP/ASPI public report on AI and human-machine teaming for intelligence analysis, routed for governance, training, and analytic-workflow boundary discussion.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[McMahon, 2024]	Analytic Tradecraft Standards in an Age of AI	curriculum_anchor	analytic_tradecraft_standards	primary_evidence	2026-06-15	annual	analyst, tradecraft reviewer, AI governance reviewer, instructor	ICD 203 and AI-tool review, analyst-ownership checklist design, and tradecraft standards caveats	analytic objectivity, accountability, civil liberties, public confidence, and human responsibility	Belfer Center Intelligence Project report on how AI tools interact with analytic tradecraft standards, especially source distinction, alternatives, uncertainty, and analyst ownership.
[et al., 2019]	Analysis of Competing Hypotheses in Intelligence Analysis	curriculum_anchor	evaluation_validity	peer_reviewed	2026-06-15	annual	analyst, method instructor, reviewer, red-team facilitator	ACH method evidence review, SAT caveat writing, and analytic-bias classroom comparison	analytic fairness, uncertainty communication, cognitive-bias awareness, and accountable review	Applied Cognitive Psychology article on Analysis of Competing Hypotheses in intelligence analysis, routed as empirical/SAT evidence with explicit limitations.
[et al., 2024b]	Task Structure, Confirmation Bias, and the Generation of Alternative Hypotheses	curriculum_anchor	evaluation_validity	peer_reviewed	2026-06-15	annual	method instructor, analyst, reviewer, learner	confirmation-bias negative-control design, alternative-hypothesis checklist review, and task-structure caveats	analytic fairness, cognitive-bias mitigation, transparent alternatives, and reviewer challenge	Cognitive Research article on how task structure affects confirmation bias and alternative hypotheses, useful for designing negative controls around ACH and SAT exercises.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[The White House, 1988]	National Operations Security Program, NSDD 298	curriculum_anchor	cognitive_influence	official_publication	2026-06-15	biennial	instructor, OPSEC reviewer, collection-governance reviewer	OPSEC doctrine provenance review, critical-information boundary setting, and defensive classroom governance	lawful authority, source protection, public safety, records accountability, and evidence-bounded education	National Security Decision Directive 298 establishing national operations security program policy, used as public historical doctrine context for defensive OPSEC governance.
[Wardle and Derakhshan, 2017]	Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making	curriculum_anchor	cognitive_influence	public_domain_publication	2026-06-15	annual	media-literacy instructor, cognitive-security reviewer, policy analyst	information-disorder taxonomy review, provenance checklist design, and cognitive-security rights caveats	freedom of expression, public trust, media literacy, privacy, and non-censorial resilience education	Council of Europe report providing an interdisciplinary framework for information disorder, routed as terminology and source-provenance support for defensive cognitive-security lessons.
[Deng and UNIDIR, 2023]	Exploring Synthetic Data for Artificial Intelligence and Autonomous Systems	curriculum_anchor	model_data	public_domain_publication	2026-06-15	annual	AI governance reviewer, data steward, instructor, policy analyst	synthetic-data risk review, AI-DSS dataset-provenance caveats, and autonomous-systems governance framing	lawful use, safety, data integrity, bias, human oversight, and international-security responsibility	UNIDIR primer on synthetic data for artificial intelligence and autonomous systems, used for source-quality and risk caveats around synthetic fixtures and military AI governance.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[for Strategic and Studies, 2022]	Crossing the Deepfake Rubicon	curriculum_anchor	synthetic_media_provenance	primary_domain_or_official	2026-06-15	annual	cognitive-security reviewer, policy analyst, instructor	deepfake risk governance, policy brief caveats, and synthetic-media threat-boundary review	identity integrity, public trust, consent, democratic resilience, and non-manipulative education	CSIS public analysis on deepfake risk as a policy and security concern, routed to synthetic-media provenance and cognitive-security safeguards.
[National Security Agency et al., 2023]	Contextualizing Deepfake Threats to Organizations	curriculum_anchor	synthetic_media_provenance	official_primary	2026-06-15	semiannual	cyber defender, cognitive-security reviewer, instructor, communications reviewer	deepfake-threat defensive control review, provenance triage, and public-sector awareness caveats	identity protection, trust, privacy, safety, and defensive awareness	Joint Cybersecurity Information Sheet on contextualizing deepfake threats, routed as official defensive guidance for provenance and synthetic-media risk review.
[Agency, 2017a]	Active Social Engineering Defense	curriculum_anchor	cyber_threat_intelligence	official_primary	2026-06-15	annual	cyber defender, instructor, social-engineering defense reviewer	social-engineering defense boundary, adversarial-interaction ethics review, and cyber-resilience classroom caveats	defensive security, consent, transparency, privacy, and protection from manipulation	DARPA public program page for Active Social Engineering Defense, used as official defensive context for social-engineering resilience and automation-risk caveats.
[et al., 2015]	Active Inference and Epistemic Value	curriculum_anchor	cognitive_active_inference	scholarly_peer_reviewed	2026-06-15	annual	theory reviewer, instructor, method designer	active-inference theory boundary, epistemic-value caveat, and formal-source review	epistemic humility, transparent analogy, scientific caveat, and human accountability	PubMed-indexed active-inference source on epistemic value, routed as theory support for bounded analogies in the cognitive-active-inference profile.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[et al., 2017]	Uncertainty, Epistemics and Active Inference	curriculum_anchor	cognitive_actsci	scholarly_peer	2026-06-15	annual	theory reviewer, instructor, governance reviewer	active-inference uncertainty caveat, theory-to-analogy review, and non-overclaiming checks	scientific transparency, epistemic humility, human accountability, and non-deceptive explanation	Open-access PMC article on uncertainty, epistemics, and active inference, encoded for theory boundaries and claim-calibration around active-inference analogies.
[et al., 2022]	A Step-by-Step Tutorial on Active Inference and Its Application to Empirical Data	curriculum_anchor	cognitive_actsci	scholarly_peer	2026-06-15	annual	learner, theory instructor, method reviewer	active-inference tutorial review, implementation-analogy caveat, and learner-facing theory learning support	scientific transparency, learner comprehension, accessibility, and non-overclaiming	Open-access tutorial on active inference and empirical-data applications, routed as a learner-facing formal-method source for bounded AGEINT analogies.
[et al., 2021a]	Active Inference in Modeling Conflict	curriculum_anchor	cognitive_actsci	scholarly_peer	2026-06-15	annual	theory reviewer, instructor, simulation-method reviewer	active-inference conflict-modeling boundary, simulation caveat, and theory-to-scenario review	non-escalatory education, scientific transparency, human accountability, and avoidance of live targeting	Zenodo-hosted scholarly source on active inference in modeling conflict, used only for bounded theory-to-scenario analogies and caveated simulation discussion.
[Kozera, 2020]	Fitness OSINT: Identifying and Tracking Military and Security Personnel with Fitness Applications	curriculum_anchor	osint_geoint	scholarly_peer	2026-06-15	annual	OSINT instructor, privacy reviewer, assurance reviewer	OSINT privacy-risk review, fitness-app leakage classroom caveat, and public-source minimization checklist	privacy, physical safety, minimization, consent, and protection from live tracking	Security and Defence article on identifying and tracking military and security personnel through fitness-app data, routed as a privacy and source-minimization warning.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[et al., 2025b]	Adversarial Machine Learning in Cybersecurity	curriculum_anchor	red_team_assurance	scholarly_peer_reviewed	2026-06-15	annual	AI security reviewer, cyber instructor, red-team reviewer	adversarial-ML literature review, cyber-AI control mapping, and defensive testing caveats	security, system integrity, safety, accountable testing, and defensive education	Journal article reviewing adversarial machine learning in cybersecurity, encoded as supplemental scholarly support for defensive AI red-team assurance.
[et al., 2023b]	Challenges of Artificial Intelligence to Cognitive Security and Safety	curriculum_anchor	cognitive_influence_security	scholarly_peer_reviewed	2026-06-15	annual	cognitive-security reviewer, instructor, AI safety reviewer	cognitive-security risk caveat, AI safety source routing, and resilience-evidence calibration	mental autonomy, safety, public trust, transparency, and non-manipulative resilience education	Open-access Safety and Security article on AI challenges to cognitive security and safety, routed as bounded cognitive-security risk context.
[Deppe and Schaal, 2024]	A Conceptual Framework and Method for a NATO ACT Concept for Cognitive Warfare	curriculum_anchor	cognitive_influence_security	scholarly_peer_reviewed	2026-06-15	annual	cognitive-security reviewer, policy instructor, assurance reviewer	NATO cognitive-warfare concept caveat, influence-risk framing, and evidence-bounded classroom boundary	mental autonomy, democratic accountability, public trust, and non-manipulative education	Open-access PMC article on a NATO ACT cognitive-warfare concept, routed for conceptual and governance framing with explicit evidence-bounded limits.
[Terp and Breuer, 2022]	DISARM: A Framework for Analysis of Disinformation Campaigns	curriculum_anchor	cognitive_influence_security	scholarly_peer_reviewed	2026-06-15	annual	cognitive-security analyst, instructor, incident reviewer	DISARM taxonomy review, defensive influence-incident mapping, and provenance checklist design	transparency, public trust, freedom of expression, privacy, and defensive resilience	IEEE source on the DISARM framework for disinformation and influence operations, used for defensive taxonomy and reviewable incident mapping.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[et al., 2024c]	Large Language Models and Disinformation: A Double-Edged Sword	curriculum_analyst	cognitive_influence_security	scholarly_peer_reviewed	2026-06-15	annual	cognitive-security reviewer, AI safety reviewer, instructor	LLM disinformation risk review, model-misuse caveats, and defensive detection limits	information integrity, democratic trust, transparency, privacy, and non-manipulative education	IEEE article on large language models and disinformation, routed as risk-and-defense context with explicit no-generation and no-campaign boundaries.
[et al., 2025c]	Large Language Models Can Generate Election Disinformation	curriculum_analyst	cognitive_influence_security	scholarly_peer_reviewed	2026-06-15	annual	cognitive-security reviewer, election-integrity educator, AI governance reviewer	election-disinformation caveat, LLM risk boundary, and public-impact review	democratic participation, information integrity, transparency, and public trust	Open-access PMC article on LLM-generated election disinformation, routed as public-impact evidence for defensive cognitive-security education.
[et al., 2023c]	Fighting Fire with Fire: Using Large Language Models to Combat Disinformation	curriculum_analyst	cognitive_influence_security	scholarly_peer_reviewed	2026-06-15	annual	AI evaluator, cognitive-security reviewer, instructor	LLM-based disinformation detection caveat, defensive NLP review, and method-limit discussion	free expression, transparency, fairness, accountable moderation, and detection-limit communication	ACL EMNLP paper on using large language models for disinformation detection, routed as defensive method evidence with explicit reliability and rights caveats.
[Farid and Bohacek, 2022]	Protecting World Leaders Against Deep Fakes	curriculum_analyst	synthetic_media_provenance	scholarly_peer_reviewed	2026-06-15	annual	cognitive-security reviewer, communications reviewer, instructor	deepfake-protection caveat, public-figure identity risk review, and synthetic-media provenance safeguards	identity integrity, consent, democratic trust, public safety, and non-manipulative education	Open-access PMC article on protecting world leaders against deepfakes, routed as identity-integrity and provenance-risk support for defensive education.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[et al., 2020]	Human Cognition Through the Lens of Social Engineering Cyberattacks	curriculum_analyst	cognitive_influence_security	scholarly_preprint	2026-06-15	annual	security-awareness instructor, cognitive-security reviewer, cyber defender	social-engineering cognition review, defensive awareness framing, and no-playbook safety boundary	privacy, consent, user protection, psychological safety, and defensive education	Open-access PMC article on human cognition in social-engineering cyberattacks, routed as defensive awareness and cognitive-security evidence with operational details excluded.
[et al., 2021b]	Situation Awareness in Intelligence Scenarios	curriculum_analyst	analytic_cognition	scholarly_preprint	2026-06-15	annual	analyst, instructor, cognitive-workload reviewer	situation-awareness scenario review, analyst-cognition caveats, and intelligence-training source support	analyst comprehension, transparency, cognitive workload, and accountable training	Open-access PMC article on situation awareness in intelligence scenarios, useful for analytic-cognition lessons and scenario-review vocabulary.
[et al., 2024d]	AI Emergency Preparedness	curriculum_analyst	agent_incident_response	scholarly_preprint	2026-06-15	semiannual	incident commander, AI governance reviewer, instructor, tabletop facilitator	AI emergency-preparedness tabletop caveat, incident-readiness review, and public-safety boundary setting	public safety, accountability, transparency, due process, and incident learning	arXiv preprint on AI emergency preparedness, routed to agent incident-response and publication-readiness caveats for tabletop exercises.
[et al., 2025a]	The AI Incident Regime	curriculum_analyst	agent_incident_response	scholarly_preprint	2026-06-15	semiannual	AI incident reviewer, legal/oversight reviewer, instructor, risk owner	AI incident-regime comparison, governance-exception review, and reporting-system caveats	transparency, accountability, due process, public safety, and affected-party protection	arXiv HTML source on AI incident regimes, routed as comparative governance context for incident reporting, risk exceptions, and assurance evidence.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Cooper, 2005]	Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis	curriculum_anchor	analytic_tradecraft	official_primary	2026-06-15	annual	analytic tradecraft instructor; curriculum designer; reviewer	Adds institutional self-critique to SAT evidence boundaries and analytic process reform lessons.	public CIA CSI monograph used for education and source-backed critique	CIA Center for the Study of Intelligence monograph on analytic pathologies, self-correction, and intelligence-process reform.
[Janis, 1982]	Groupthink: Psychological Studies of Policy Decisions and Fiascoes	curriculum_anchor	analytic_cognition	scholarly_book	2026-06-15	annual	analytic tradecraft instructor; cognition reviewer; curriculum designer	Keeps group-process lessons tied to a named scholarly source while preserving caveats about retrospective failure explanation.	copyrighted scholarly book metadata only; cite and summarize sparingly	Scholarly book record for Janis's groupthink model used as classic context for dissent, alternatives, and group-decision failure claims.
[Coulthart, 2016]	Why Do Analysts Use Structured Analytic Techniques? An In-depth Study of an American Intelligence Agency	curriculum_anchor	sat_evaluation	scholarly_peer_reviewed	2026-06-15	annual	curriculum designer; analytic standards trainer; evaluation lead	Separates usage and institutionalization evidence from efficacy evidence in SAT lessons.	copyrighted scholarly article; cite DOI metadata and summarize sparingly	Peer-reviewed study of why analysts use SATs, supporting adoption, training, and organizational-context claims rather than universal efficacy claims.
[Coulthart, 2017]	An Evidence-Based Evaluation of 12 Core Structured Analytic Techniques	curriculum_anchor	sat_evaluation	scholarly_peer_reviewed	2026-06-15	annual	curriculum designer; analytic standards trainer; evaluation lead	Forces SAT exercises to distinguish doctrine, classroom utility, and empirical support by technique.	copyrighted scholarly article; cite DOI metadata and summarize sparingly	Peer-reviewed evaluation of core SATs used to qualify claims about where specific techniques may or may not have evidence support.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Tetlock, 2018]	Restructuring Structured Analytic Techniques in Intelligence	curriculum_anchor	evaluation	scholarly_evidence	2026-06-15	annual	curriculum designer; analytic standards trainer; evaluation lead	Connects SAT chapter revisions to decision-science evidence and claim-calibration gates.	copyrighted scholarly article; cite DOI metadata and summarize sparingly	Peer-reviewed article arguing for a more evidence-attentive structuring of SATs and stronger links to judgment and decision-science research.
[Whitesmith, 2019]	The Efficacy of ACH in Mitigating Serial Position Effects and Confirmation Bias in an Intelligence Analysis Scenario	curriculum_anchor	evaluation	scholarly_evidence	2026-06-15	annual	curriculum designer; analytic standards trainer; cognition reviewer	Prevents ACH lessons from turning one experimental result into a universal debiasing assertion.	copyrighted scholarly article; cite DOI metadata and summarize sparingly	Peer-reviewed ACH experiment used to keep confirmation-bias and serial-position claims specific to a study design rather than a general SAT guarantee.
[Mandel, 2020]	Coherence of Probability Judgments from Uncertain Evidence: Does ACH Help?	curriculum_anchor	evaluation	scholarly_evidence	2026-06-15	annual	curriculum designer; forecasting instructor; analytic standards trainer	Anchors manuscript language that separates ACH transparency from accuracy or coherence proof.	open scholarly article; cite source and avoid extended quotation	Open Cambridge article testing whether ACH improves coherence of probabilistic judgments from uncertain evidence.
[Dhami, 2018]	Boosting Intelligence Analysts' Judgment Accuracy: What Works, What Fails?	curriculum_anchor	forecasting_calibration	scholarly_evidence	2026-06-15	annual	forecasting instructor; curriculum designer; evaluation lead	Routes SAT automation claims toward accountable judgment support, not analyst replacement.	open scholarly article; cite source and avoid extended quotation	Open Judgment and Decision Making article comparing ACH, coherentization, and aggregation for intelligence analysts' probability judgments.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Tetlock, 2015b]	Improving Intelligence Analysis With Decision Science	curriculum_anchor	forecasting_calibration	scholarly_peer_reviewed	2026-06-15	annual	forecasting instructor; evaluation lead; curriculum designer	Gives the SAT chapter an evidence complement beyond technique catalogues and post-mortem lessons.	copyrighted scholarly article; cite DOI metadata and summarize sparingly	Peer-reviewed decision-science article connecting intelligence analysis improvement to forecasting, probability judgment, and uncertainty communication evidence.
[Council, 2011]	Intelligence Analysis for Tomorrow: Advances from the Behavioral and Social Sciences	curriculum_anchor	analytic_cognition	scholarly_publication_report	2026-06-15	annual	curriculum designer; cognition reviewer; evaluation lead	Links analytic-cognition lessons to a public expert-report baseline and keeps SAT claims evidence-sensitive.	National Academies publication metadata and public report access; cite and summarize sparingly	National Academies report connecting behavioral and social science to intelligence-analysis training, judgment, and organizational improvement.
[on Intelligence, 2004]	Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq	curriculum_anchor	intelligence_failure	official_publication_report	2026-06-15	biennial	curriculum designer; governance reviewer; analytic tradecraft instructor	Prevents failure lessons from implying that any single SAT would have prevented a complex institutional failure.	public-domain government report; cite official source	Official Senate report on prewar Iraq intelligence assessments used as post-mortem context for assumptions, dissent, caveats, and source-confidence failures.
[Activity, 2010]	Aggregative Contingent Estimation	curriculum_anchor	forecasting_calibration	official_publication_program_page	2026-06-15	annual	forecasting instructor; curriculum designer; evaluation lead	Connects SAT lessons to calibration and aggregation evidence without claiming autonomous forecasting judgment.	public IARPA program metadata used for education and source-backed synthesis	Official IARPA ACE program page on eliciting, weighting, and combining probabilistic judgments to improve intelligence forecasts.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Activity, 2023]	Rapid Explanation, Analysis and Sourcing Online	curriculum_anchor	agentic_analytic_assistance	official_program	2026-06-15	annual	analytic method designer; AI governance reviewer; curriculum designer	Constrains AI/SAT automation prose away from autonomous strategic judgment, targeting, or report replacement.	public IARPA program metadata used for education and governance review	Official IARPA REASON program page on analyst-in-the-loop evidence and reasoning support for draft analytic reports.
[Helmer, 1963]	An Experimental Application of the DELPHI Method to the Use of Experts	curriculum_anchor	forecasting_calibration	scholarly_peer_reviewed	2026-06-15	annual	forecasting instructor; methods instructor; curriculum designer	Adds historical method roots for aggregation and structured elicitation exercises.	copyrighted scholarly article; cite DOI metadata and summarize sparingly	Classic peer-reviewed Delphi-method article used as historical method context for structured expert elicitation and iterative judgment aggregation.
[Klein, 2007]	Performing a Project Premortem	curriculum_anchor	analytic_methodology	professional_pedagogy	2026-06-15	annual	methods instructor; curriculum designer; reviewer	Adds a named structured failure-review technique while retaining explicit evidence limits.	copyrighted professional article; cite metadata and summarize sparingly	Professional practice article introducing the premortem as a structured way to surface possible failure causes before commitment.
[Marrin, 2012]	Improving Intelligence Analysis: Bridging the Gap between Scholarship and Practice	curriculum_anchor	analytic_methodology	scholarly_pedagogy	2026-06-15	annual	curriculum designer; intelligence-studies instructor; methods reviewer	Connects SAT integration to a broader scholarship-practice gap rather than technique cataloging alone.	copyrighted scholarly book metadata only; cite and summarize sparingly	Routledge scholarly book on linking intelligence-analysis scholarship and practice, used for tradecraft pedagogy and evidence-uptake framing.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Svenmarck, 2021]	Overview of Structured Analytic Techniques for Assessment and Judgement of Major Events	curriculum_author	analytic_method	official_report	2026-06-15	annual	curriculum designer; public-sector method instructor; reviewer	Adds a non-US official SAT training reference while keeping efficacy claims separate from technique catalog coverage.	public official report summary; cite source and avoid extended quotation	Swedish Defence Research Agency report summary on 42 structured analytic techniques for assessment and judgement of major events.
[Service, 2021]	Technical Brief on Joint Structured Analysis Techniques	curriculum_author	analytic_method	public_pedagogy	2026-06-15	annual	methods instructor; curriculum designer; collaborative-analysis facilitator	Broadens SAT pedagogy beyond intelligence-only settings while preserving domain and efficacy caveats.	public guidance page; cite source and avoid extended quotation	JIPS technical brief on joint structured analysis techniques for collaborative humanitarian and development data analysis.
[Denzler, 2024]	Revisiting the Psychology of Structured Analytical Techniques	curriculum_author	analytic_cognition	scholarly_peer_reviewed	2026-06-15	annual	cognition reviewer; analytic standards trainer; curriculum designer	Keeps cognitive-security and tradecraft prose explicit about mechanism uncertainty and evidence limits.	copyrighted scholarly article; cite DOI metadata and summarize sparingly	Peer-reviewed article revisiting psychological assumptions behind SATs and their relationship to analytic cognition.
[Mandel, 2024]	Critical Review of the Analysis of Competing Hypotheses Technique: Lessons for the Intelligence Community	curriculum_author	evaluation_validity	scholarly_peer_reviewed	2026-06-15	annual	analytic standards trainer; curriculum designer; evaluation lead	Strengthens SAT chapter language that separates hypothesis bookkeeping, diagnosticity review, and accuracy evidence.	copyrighted scholarly article; cite DOI metadata and summarize sparingly	Peer-reviewed critical review of ACH used to frame ACH as a diagnostic and review aid with contested efficacy claims.
[Miksa, 2024]	Assessment Tabling: An Integrated Structured Analytic Technique for Improved Intelligence Analysis and Reasoning Visualisation	curriculum_author	analytic_method	scholarly_peer_reviewed	2026-06-15	annual	methods instructor; visualization reviewer; curriculum designer	Feeds figure-caption and classroom-artifact language about visible reasoning without calling the visual a score.	copyrighted scholarly article; cite DOI metadata and summarize sparingly	Peer-reviewed article proposing assessment tabling as an integrated SAT and reasoning-visualization approach.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Coulthart, 2025]	Structured Analytic Techniques in an Intelligence Fusion Centre: A Survey of Analyst Perspectives and Use	curriculum_anchor	evaluation_evidence	scholarly_peer_reviewed	2026-06-15	annual	curriculum designer; analytic standards trainer; evaluation lead	Adds current practice evidence while keeping adoption, perception, and efficacy as separate claims.	copyrighted scholarly article; cite DOI metadata and summarize sparingly	Peer-reviewed survey of SAT perspectives and use in an intelligence fusion-centre context, useful for adoption and training caveats.
[Gustafson, 2025]	Teaching Structured Analytic Techniques across Nations: Same, Same but Different	curriculum_anchor	analytic_method	scholarly_peer_reviewed	2026-06-15	annual	curriculum designer; analytic tradecraft instructor; pedagogy reviewer	Strengthens AGEINT's classroom framing and local-context caveats for SAT exercises.	copyrighted scholarly article; cite DOI metadata and summarize sparingly	Peer-reviewed article on cross-national SAT teaching used for pedagogy, transfer, and local-context caveats.
[McCarthy, 2024]	Seeing the Futures: Evaluating the Application of Structured Analytic Technique Alternative Futures Analysis	curriculum_anchor	warning_intelligence	scholarly_peer_reviewed_open	2026-06-15	annual	warning instructor; curriculum designer; methods reviewer	Improves AFA and warning lessons without claiming scenario exercises predict the future.	open journal page; cite source and avoid extended quotation	National Security Journal article evaluating Alternative Futures Analysis as an imaginative-thinking SAT and emphasizing purpose-fit and facilitator context.
[Ritchey, 2013]	General Morphological Analysis: A General Method for Non-Quantified Modelling	curriculum_anchor	analytic_method	public_pedagogy	2026-06-15	annual	methods instructor; curriculum designer; visualization reviewer	Adds method-root support for morphological and scenario matrix exercises while preserving review gates.	public method page; cite source and avoid extended quotation	Swedish Morphological Society page explaining general morphological analysis as a method for structuring non-quantified complex problem spaces.
[Pherson, 2014b]	Cases in Intelligence Analysis: Structured Analytic Techniques in Action	curriculum_anchor	analytic_method	scholarly_pedagogy	2026-06-15	annual	curriculum designer; analytic tradecraft instructor; pedagogy reviewer	Adds publisher-backed support for SAT classroom-artifact language and exercise design.	copyrighted textbook metadata only; cite and summarize sparingly	SAGE/CQ Press textbook page for SAT case pedagogy and classroom exercises for analyst training.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Pherson, 2020]	Critical Thinking for Strategic Intelligence	curriculum_anchor	analytic_methodology	scholarly_pedagogy	2026-06-15	annual	curriculum designer; analytic tradecraft instructor; writing reviewer	Strengthens SAT-adjacent teaching language around critical questions, source evaluation, and accountable presentation.	copyrighted textbook metadata only; cite and summarize sparingly	SAGE/CQ Press textbook page for critical-thinking questions, analytic techniques, uncertainty, graphics, and source evaluation in intelligence education.
[of the Army., 2006]	FM 2-22.3 Human Intelligence Collector Operations	curriculum_anchor	humint_doctrine	official_primary	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that humint_doctrine claims stay source-backed, bounded, and separated from operational practice.	public-source record; education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for humint_doctrine; routed to HUMINT collection discipline; source operations; interrogation ethics and doctrine. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[of the Director of National Intelligence., 2008]	ICD 304: Human Intelligence	curriculum_anchor	humint_doctrine	official_primary	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that humint_doctrine claims stay source-backed, bounded, and separated from operational practice.	public-source record; education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for humint_doctrine; routed to HUMINT governance; IC collection management; CI integration. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of the Director of National Intelligence., 2016]	ICD 310: Coordination of Clandestine Human Source Collection Outside the US	curriculum_anchor	humint_doctrine	official_primary	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that humint_doctrine claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for humint_doctrine; routed to HUMINT deconfliction; CI integration; overseas collection coordination. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[to Study Governmental Operations with Respect to Intelligence Activities, Church Committeea]	Church Committee Final Report Book I: Foreign and Military Intelligence (S. Rep. 94-755)	curriculum_anchor	humint_oversight_history	public_domain_primary	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that humint_oversight_history claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified public domain primary source for humint_oversight_h routed to HUMINT history and oversight; IC accountability; CI doctrine history. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[to Study Governmental Operations with Respect to Intelligence Activities, Church Committeeb]	Church Committee Book III: NSA Surveillance (S. Rep. 94-755)	curriculum_anchor	sigint_oversight_history	public_domain_primary	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that sigint_oversight_history claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified public domain primary source for sigint_oversight_histor routed to SIGINT oversight history; NSA authorities and limitations; domestic surveillance doctrine. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[of the Director of National Intelligence., 2007]	ICD 302: Document and Media Exploitation	curriculum_anchor	humint_doctrine	official_primary	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that humint_doctrine claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for humint_doctrine; routed to HUMINT collection; document and media analyzeation; all-source integration. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of the Joint Chiefs of Staff., 2012]	JP 2-01: Joint and National Intelligence Support to Military Operations (2012)	curriculum_anchor	collection_management_doctrine	official_primary	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that collection_management_doctrine claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for collection_management_doctrine routed to All-source collection management; HUMINT/SIGINT/GEOINT integration; joint intelligence support. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Agency., n.d.]	TEMPEST: A Signal Problem (NSA Declassified)	curriculum_anchor	sigint_emanations_intelligence	official_primary	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that sigint_emanations_intelligence claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for sigint_emanations_intelligence routed to SIGINT fundamentals; emanations intelligence; EMSEC/TEMPEST history. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[National Security Agency, Various years]	NSA Center for Cryptologic History: Historical Publications	curriculum_anchor	sigint_history	official_primary	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that sigint_history claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for sigint_history; routed to SIGINT history; NSA organizational development; cryptologic heritage; ELINT/TELINT history. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[of Standards and Technology., 2024a]	FIPS 203: ML-KEM Post-Quantum Key-Encapsulation Standard	curriculum_anchor	cryptography_standards	official_primary	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that cryptography_standards claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for cryptography_standards; routed to Cryptography standards; post-quantum SIGINT resilience; communications security modernization. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of Standards and Technology., 2024b]	FIPS 204: ML-DSA Post-Quantum Digital Signature Standard	curriculum_anchor	cryptography_standards	official_publication	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that cryptography_standards claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for cryptography_standards; routed to Cryptography standards; post-quantum digital signatures; authentication in collection systems. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[of Standards and Technology., 2024c]	FIPS 205: SLH-DSA Post-Quantum Hash-Based Signature Standard	curriculum_anchor	cryptography_standards	official_publication	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that cryptography_standards claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for cryptography_standards; routed to Cryptography standards; post-quantum signature diversity; long-term data integrity. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Office of the Director of National Intelligence, 2022]	ODNI Declassified Report on Commercially Available Information (2022)	curriculum_anchor	osint_doctrine	official_primary	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that osint_doctrine claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for osint_doctrine; routed to OSINT/PAI doctrine; commercially available information; privacy and civil liberties in collection. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[of the Joint Chiefs of Staff., 2017]	JP 2-03: Geospatial Intelligence in Joint Operations (2017)	curriculum_anchor	geoint_doctrine	official_primary	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that geoint_doctrine claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for geoint_doctrine; routed to GEOINT doctrine; imagery intelligence in joint operations; NGA role; GEOINT organizations. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Clark, 2020]	Geospatial Intelligence: Origins and Evolution (Georgetown UP, 2020)	curriculum_anchor	geoint_tradecraft	scholarly_book_metadata	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that geoint_tradecraft claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly book metadata source for geoint_tradecraft; routed to GEOINT history and doctrine; remote sensing intelligence; IMINT tradecraft. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Van Puyvelde, 2025]	The rise of open-source intelligence, EJIS 2025	curriculum_anchor	osint_methodology	scholarly_repository_record	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that osint_methodology claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly repository record source for osint_methodology; routed to OSINT definition and discipline; OSINT methodology; validation and verification; civil society OSINT. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of the Director of National Intelligence., Current]	ICD 206: Sourcing Requirements for Disseminated Analytic Products (with ICS 206-01 on PAI/CAI/OSINT)	curriculum_anchor	osint_doctrine	official_primary	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that osint_doctrine claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for osint_doctrine; routed to OSINT sourcing standards; analytic product integrity; IC information sourcing discipline. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Agency., 2018]	NGA Pub 1.0: GEOINT Basic Doctrine (2018)	curriculum_anchor	geoint_doctrine	official_primary	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that geoint_doctrine claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for geoint_doctrine; routed to GEOINT doctrine; NGA mission; GEOINT principles and definitions. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of the Director of National Intelligence., 2024]	ODNI Commercially Available Information Fact Sheet (May 2024)	curriculum_anchor	osint_doctrine	official_primary	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that osint_doctrine claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for osint_doctrine; routed to OSINT/PAI governance; CAI policy framework; privacy in collection. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Hutchins, 2011]	Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains	curriculum_anchor	cyber_threat_intelligence	professional_documentation	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that cyber_threat_intelligence claims stay source-backed, bounded, and separated from operational practice.	public-source intelligence, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified professional documentation source for cyber_threat_intellige routed to Cyber Intelligence Fundamentals; APT Threat Intelligence; Structured Analytic Techniques for Cyber. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Caltagirone, 2013]	The Diamond Model of Intrusion Analysis	curriculum_anchor	cyber_threat_intelligence	professional_documentation	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that cyber_threat_intelligence claims stay source-backed, bounded, and separated from operational practice.	public-source intelligence, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified professional documentation source for cyber_threat_intelligence routed to Cyber Intelligence Fundamentals; APT Analysis; Structured Analytic Techniques for Cyber CTI. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[CISA, 2024]	PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure (AA24-038A)	curriculum_anchor	apt_threat_intelligence	official_primary	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that apt_threat_intelligence claims stay source-backed, bounded, and separated from operational practice.	public-source intelligence, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for apt_threat_intelligence routed to Advanced Persistent Threats; ICS/OT Threat Intelligence; Supply Chain and Critical Infrastructure. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[NSA, 2023]	PRC State-Sponsored Cyber Actor Living off the Land to Evade Detection (AA23-144A)	curriculum_analyst	apt_threat_intelligence	official_primary	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that apt_threat_intelligence claims stay source-backed, bounded, and separated from operational practice.	public-source intelligence, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for apt_threat_intelligence routed to Advanced Persistent Threats; Cyber Intelligence Fundamentals; ICS/OT Security. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[DOE, 2022]	APT Cyber Tools Targeting ICS/SCADA Devices (AA22-103A)	curriculum_analyst	apt_threat_intelligence	official_primary	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that apt_threat_intelligence claims stay source-backed, bounded, and separated from operational practice.	public-source intelligence, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for apt_threat_intelligence routed to Advanced Persistent Threats; ICS/OT Security; MITRE ATT&CK for ICS. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[CISA., 2020]	Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations (AA20-352A)	curriculum_analyst	supply_chain_intelligence	official_primary	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that supply_chain_intelligence claims stay source-backed, bounded, and separated from operational practice.	public-source intelligence, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for supply_chain_intelligence routed to Supply Chain Intelligence Attacks; Advanced Persistent Threats; Threat Intelligence Sharing. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Lee, 2016]	Analysis of the Cyber Attack on the Ukrainian Power Grid	curriculum_anchor	historical_ics_incidents	official_primary	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that historical_ics_incidents claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for historical_ics_incidents; routed to Historical ICS Cyber Incidents; ICS/OT Security; Threat Intelligence Sharing for Critical Infrastructure. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[for Cybersecurity, ENISA]	ENISA Threat Landscape 2024	curriculum_anchor	cyber_threat_intelligence	official_primary	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that cyber_threat_intelligence claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for cyber_threat_intellige routed to Cyber Intelligence Fundamentals; Advanced Persistent Threats; ICS/OT Security; Threat Intelligence Sharing. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Boyens, 2022]	Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (NIST SP 800-161 Rev. 1)	curriculum_analyst	supply_chain_intelligence	official_primary	2026-04-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that supply_chain_intelligence claims stay source-backed, bounded, and separated from operational practice.	public-source collection, attribution-accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for supply_chain_intelligen routed to Supply Chain Intelligence Attacks; ICS/OT Security; Threat Intelligence Sharing. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Biden, 2021]	Executive Order 14028 on Improving the Nation's Cybersecurity	curriculum_analyst	supply_chain_intelligence	official_primary	2026-04-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that supply_chain_intelligence claims stay source-backed, bounded, and separated from operational practice.	public-source collection, attribution-accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for supply_chain_intelligen routed to Supply Chain Intelligence Attacks; Cyber Intelligence Fundamentals; ICS/OT Security. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of Incident Response and Teams, FIRST]	Traffic Light Protocol (TLP) — FIRST Standards Definitions and Usage Guidance, Version 2.0	curriculum_anchor	threat_intel_sharing_standards	official_primary	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that threat_intel_sharing_standards claims stay source-backed, bounded, and separated from operational practice.	public-source only; accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for threat_intel_sharing routed to Threat Intelligence Sharing for Critical Infrastructure; Cyber Intelligence Fundamentals. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Corporation, NERC]	NERC CIP Reliability Standards (CIP-002 through CIP-015)	curriculum_anchor	ics_ot_security_standards	official_primary	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that ics_ot_security_standards claims stay source-backed, bounded, and separated from operational practice.	public-source only; accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for ics_ot_security_sta routed to ICS/OT Security; Critical Infrastructure Protection; Threat Intelligence Sharing for Critical Infrastructure. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Cherepanov, 2017]	Win32/Industroyer: A New Threat for Industrial Control Systems	curriculum_anchor	historical_ics_incidents	professional_documentation	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that historical_ics_incidents claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified professional documentation source for historical_ics_incidents; routed to Historical ICS Cyber Incidents; ICS/OT Security; MITRE ATT&CK for ICS. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[ICS-CERT., 2010]	ICSA-10-272-01: Stuxnet Malware Mitigation	curriculum_anchor	historical_ics_incidents	official_primary	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that historical_ics_incidents claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for historical_ics_incidents; routed to Historical ICS Cyber Incidents; ICS/OT Security; MITRE ATT&CK for ICS. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[CISA., 2022]	Control System Defense: Know the Opponent	curriculum_anchor	ics_ot_security_standards	official_primary	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that ics_ot_security_standards claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for ics_ot_security_sta routed to ICS/OT Security; Advanced Persistent Threats; MITRE ATT&CK for ICS. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[ICS., 2017]	ICS Defense Use Case No. 6: Modular ICS Malware	curriculum_anchor	historical_ics_incidents	official_primary	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that historical_ics_incidents claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for historical_ics_incidents; routed to Historical ICS Cyber Incidents; ICS/OT Security; MITRE ATT&CK for ICS. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[for Network and Security, ENISA]	Protecting Industrial Control Systems: Recommendations for Europe and Member States	curriculum_anchor	ics_ot_security_standards	official_primary	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that ics_ot_security_standards claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for ics_ot_security_sta routed to ICS/OT Security; Critical Infrastructure Protection; MITRE ATT&CK for ICS context. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of Staff., 2012]	JP 3-13, Information Operations (2012)	curriculum_anchor	information_operations_doctrine	official_primary	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that information_operations_doctrine claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for information_operations_doc routed to Information Warfare and Cognitive Security; PSYOP and MISO Doctrine. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[of Staff., 2014b]	JP 3-13.2, Military Information Support Operations (2014)	curriculum_anchor	psyop_miso_doctrine	official_primary	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that psyop_miso_doctrine claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for psyop_miso_doctrin routed to PSYOP and MISO Doctrine; Information Warfare and Cognitive Security. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Paul and Matthews., 2016]	The Russian "Firehose of Falsehood" Propaganda Model (RAND, 2016)	curriculum_anchor	active_measures_disinformation	professional_documentation	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that active_measures_disinformation claims stay source-backed, bounded, and separated from operational practice.	public-source education, account-able review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified professional documentation source for active_measures_disinformation routed to Active Measures and Disinformation; Information Warfare and Cognitive Security. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Lazer, 2018]	The science of fake news (Science, 2018)	curriculum_anchor	disinformation_misinformation	scholarly_publication	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that disinformation_misinformation claims stay source-backed, bounded, and separated from operational practice.	public-source education, account-able review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly peer reviewed source for disinformation_misinformation routed to Active Measures and Disinformation; Information Warfare and Cognitive Security; Social Engineering. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Network, FinCEN]	FinCEN SAR Narrative Guidance Package (2003/2006)	curriculum_anchor	finint_sar_reporting	official_primary	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that finint_sar_reporting claims stay source-backed, bounded, and separated from operational practice.	public-source orientation, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for finint_sar_reporting routed to Financial Intelligence (FININT). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[of Financial Intelligence Units., 2023]	Egmont Group Principles for Information Exchange Between FIUs (April 2023)	curriculum_anchor	finint_international_cooperation	official_primary	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that finint_international_cooperation claims stay source-backed, bounded, and separated from operational practice.	public-source orientation, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for finint_international_cooperation routed to Financial Intelligence (FININT). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[on Drugs and Crime, UNODC]	UNODC Money Laundering, Proceeds of Crime and the Financing of Terrorism	curriculum_anchor	finint_aml_cft_international	official_primary	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that finint_aml_cft_international claims stay source-backed, bounded, and separated from operational practice.	public-source orientation, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for finint_aml_cft_international routed to Financial Intelligence (FININT). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Schott, 2006]	World Bank/IMF Reference Guide to AML/CFT (2006)	curriculum_anchor	finint_aml_cft_international	official_publication	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that finint_aml_cft_international claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for finint_aml_cft_inte routed to Financial Intelligence (FININT). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Counterintelligence and Center, NCSCb]	National Counterintelligence Strategy 2024 (NCSC/ODNI)	curriculum_anchor	counterintelligence	official_publication	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that counterintelligence_strategy claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for counterintelligence_strategy; routed to Counterintelligence (fundamentals + against non-state actors). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Counterintelligence and Center, NCSCa]	National Counterintelligence Strategy 2020–2022 (NCSC/ODNI)	curriculum_anchor	counterintelligence	official_publication	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that counterintelligence_strategy claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for counterintelligence_strategy; routed to Counterintelligence (fundamentals + against non-state actors). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Pennycook and Rand., 2021]	The psychology of fake news (Trends in Cognitive Sciences, 2021)	curriculum_author	disinformation_cognitive_psychology	scholarly_repository_record	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that disinformation_cognitive_psychology claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly repository record source for disinformation_cognitive_psyc routed to Active Measures and Disinformation; Social Engineering; Information Warfare and Cognitive Security. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Starbird and Wilson., 2019]	Disinformation as Collaborative Work (ACM CSCW, 2019)	curriculum_author	active_measures_information_operations	scholarly_repository_record	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that active_measures_information_operations claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly repository record source for active_measures_infor routed to Active Measures and Disinformation; Information Warfare and Cognitive Security; Social Engineering. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Hoffman, 2007]	Conflict in the 21st Century: The Rise of Hybrid Wars (Potomac Institute, 2007)	curriculum_analyst	hybrid_warfare_education	scholarly_repository_record	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that hybrid_warfare_education claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly repository record source for hybrid_warfare_doctri routed to Gray Zone / Hybrid Warfare / Non-State Actor Intelligence / Irregular Warfare. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Mazarr, 2015]	Mastering the Gray Zone (USAWC Press, 2015)	curriculum_analyst	gray_zone_competition_doctrine	publication_publication_publication	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that gray_zone_competition_doctrine claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly publication metadata source for gray_zone_competit routed to Gray Zone / Hybrid Warfare / Non-State Actor Intelligence / Irregular Warfare. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[of Defense., 2020]	Irregular Warfare Annex to the National Defense Strategy – Summary (DoD, 2020)	curriculum_analyst	irregular_warfare_strategy	official_publication	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that irregular_warfare_strategy claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for irregular_warfare_strategy routed to Gray Zone / Hybrid Warfare / Non-State Actor Intelligence / Irregular Warfare. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of Staff., 2014a]	JP 3-05, Special Operations (2014)	curriculum_anchor	special_operations_doctrine	official_primary	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that special_operations_doctrine claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for special_operations_doc routed to Gray Zone / Hybrid Warfare / Non-State Actor Intelligence / Irregular Warfare; Counterintelligence. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Cialdini, 1984]	Influence: The Psychology of Persuasion (Cialdini, 1984)	curriculum_anchor	social_engineering_influence_psychology	scholarly_foundation	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that social_engineering_influence_psychology claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly metadata source for social_engineering_inf routed to Social Engineering; Active Measures and Disinformation; Information Warfare and Cognitive Security. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[of Excellence., 2021]	NATO StratCom COE Strategic Communications Hybrid Threats Toolkit (2021)	curriculum_anchor	hybrid_warfare_strategic_gray_zone	official_primary	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that hybrid_warfare_strategic_gray_zone claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for hybrid_warfare_stratc routed to Gray Zone / Hybrid Warfare / Non-State Actor Intelligence / Irregular Warfare; Active Measures and Disinformation. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[of Staff., 2013]	JP 2-0, Joint Intelligence (2013)	curriculum_anchor	imint_joint_intelligence_doctrine	official_primary	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that imint_joint_intelligence_doctrine claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for imint_joint_intellige routed to Imagery Intelligence (IMINT); Counterintelligence. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Pamment and Smith., 2022]	Attributing Information Influence Operations (NATO StratCom COE, 2022)	curriculum_anchor	active_measures_attribution	official_primary	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that active_measures_attribution claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for active_measures_attri routed to Active Measures and Disinformation; Counterintelligence; Information Warfare and Cognitive Security. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Andrew, 1990]	KGB: The Inside Story	curriculum_anchor	intelligence_history_soviet	scholarly_book	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that intelligence_history_soviet claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly book metadata source for intelligence_history_sovie routed to Historical Intelligence Services (Soviet/Russian); KGB organizational doctrine and operations overview. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Andrew, 1999]	The Sword and the Shield	curriculum_and_training	intelligence_history	scholarly_book	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that intelligence_history_claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly book metadata source for intelligence_history_soviet routed to Historical Intelligence Services (Soviet/Russian); primary-source archival history of KGB. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Andrew, 2009]	The Defence of the Realm	curriculum_and_training	intelligence_history	scholarly_book	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that intelligence_history_claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly book metadata source for intelligence_history_british_allied routed to Historical Intelligence Services (British/Allied); institutional history of domestic security intelligence. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Weiner, 2007]	Legacy of Ashes: The History of the CIA	curriculum_anchor	intelligence_history_and_memory	scholarly_publication	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that intelligence_history_and_memory claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly book metadata source for intelligence_history_and_memory routed to Historical Intelligence Services (American); CIA institutional failures and analytic dysfunction. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[to Study Governmental Operations with Respect to Intelligence Activities., 1976]	Church Committee Final Report (Internet Archive)	curriculum_anchor	legal_oversight_and_intelligence_reform	primary_publication	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that legal_oversight_and_intelligence_reform claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified public domain primary source for legal_oversight_and_intelligence_reform routed to Legal Authorities and Constraints; Historical Intelligence Services (American); oversight reform history. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Tversky, 1974]	Judgment under Uncertainty: Heuristics and Biases	curriculum_anchor	cognitive_bias_foundations	scholarly_publication	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that cognitive_bias_foundations claims stay source-backed, bounded, and separated from operational practice.	public-source education, actionable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly repository record source for cognitive_bias_foundations routed to Cognitive Security (neurocognitive mechanisms); Epistemic Rigor & Analytic Tradecraft (cognitive bias in analysis). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Kahneman, 2011]	Thinking, Fast and Slow (Wikipedia)	curriculum_anchor	cognitive_bias_foundations	scholarly_publication	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that cognitive_bias_foundations claims stay source-backed, bounded, and separated from operational practice.	public-source education, actionable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly book metadata source for cognitive_bias_foundations routed to Cognitive Security (dual-process neurocognitive mechanisms); Epistemic Rigor & Analytic Tradecraft. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Lewandowsky 2021]	Countering Misinformation through Inoculation and Prebunking	curriculum_anchor	cognitive_security_and_influence	scholarly_publication	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that cognitive_security_and_influence claims stay source-backed, bounded, and separated from operational practice.	public-source education, inoculation review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly peer reviewed source for cognitive_security_inoculation routed to Cognitive Security (psychological inoculation & prebunking); Cognitive Security Operations. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Lewandowsky 2020]	The Debunking Handbook 2020	curriculum_anchor	cognitive_security_and_influence	scholarly_publication	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that cognitive_security_and_influence claims stay source-backed, bounded, and separated from operational practice.	public-source education, inoculation review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly repository record source for cognitive_security_inoculation routed to Cognitive Security (psychological inoculation & prebunking); corrections and debunking protocol. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Pennycook, 2021]	Shifting Attention to Accuracy — Nature	curriculum_anchor	cognitive_security	scholarly_peer_reviewed	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that cognitive_security_misinformation claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly peer reviewed source for cognitive_security_misinf routed to Cognitive Security (psychological inoculation & prebunking); Cognitive Security Operations (scalable interventions). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Tetlock, 2005]	Expert Political Judgment — Internet Archive	curriculum_anchor	analytic_tradecraft	scholarly_foundational	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that analytic_tradecraft_forecasting claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly book metadata source for analytic_tradecraft_for routed to Epistemic Rigor & Analytic Tradecraft (Advanced Analysis Methods); forecasting accuracy and calibration. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Tetlock, 2015a]	Superforecasting — Google Play Books	curriculum_anchor	analytic_tradecraft_foreca	scholarly_publication	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that analytic_tradecraft_forecasting claims stay source-backed, bounded, and separated from operational practice.	public-source education; accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly book metadata source for analytic_tradecraft_for routed to Epistemic Rigor & Analytic Tradecraft (Advanced Analysis Methods); Good Judgment Project findings. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Congress., 1978]	FISA 1978 — GovInfo (Statutes at Large)	curriculum_anchor	legal_authorities_surv	official_publication	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that legal_authorities_surveillance claims stay source-backed, bounded, and separated from operational practice.	public-source education; accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for legal_authorities_surv routed to Legal Authorities and Constraints; oversight of domestic electronic surveillance. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Congress., 2001]	USA PATRIOT Act — GovInfo Compilation	curriculum_anchor	legal_authorities_surveillance	official_primary	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that legal_authorities_surveillance claims stay source-backed, bounded, and separated from operational practice.	public-source accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for legal_authorities_surv routed to Legal Authorities and Constraints; post-9/11 surveillance expansion. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Congress., 2015]	USA FREEDOM Act — GovInfo	curriculum_anchor	legal_authorities_surveillance	official_primary	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that legal_authorities_surveillance claims stay source-backed, bounded, and separated from operational practice.	public-source accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for legal_authorities_surv routed to Legal Authorities and Constraints; surveillance reform and civil liberties. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Reagan, 1981]	EO 12333 — ODNI	curriculum_anchor	legal_authorities_intelligence_collection	official_primary	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that legal_authorities_intelligence_collection claims stay source-backed, bounded, and separated from operational practice.	public-source accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official primary source for legal_authorities_inte routed to Legal Authorities and Constraints; EO-based authorities for IC collection. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Quinlan, 2007]	Just Intelligence: Prolegomena — Semantic Scholar	curriculum_anchor	ethics_of_intelligence	scholarly_repository_record	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that ethics_of_intelligence claims stay source-backed, bounded, and separated from operational practice.	public-source intelligence, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly repository record source for ethics_of_intelligence routed to Ethics of Intelligence and Cognitive Security; just-intelligence theory. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Omand, 2010]	Securing the State — Google Books	curriculum_anchor	ethics_of_intelligence	scholarly_book_record	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that ethics_of_intelligence claims stay source-backed, bounded, and separated from operational practice.	public-source intelligence, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly book metadata source for ethics_of_intelligence routed to Ethics of Intelligence and Cognitive Security; legal and ethical constraints on secret intelligence; oversight principles. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Omand, 2018]	Principled Spying — Georgetown University Press	curriculum_anchor	ethics_of_intelligence	scholarly_book_metadata	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that ethics_of_intelligence claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly book metadata source for ethics_of_intelligence routed to Ethics of Intelligence and Cognitive Security; HUMINT ethics; surveillance ethics; oversight accountability. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Russell, 2020]	Artificial Intelligence: A Modern Approach, 4th ed.	curriculum_anchor	agent_foundations	scholarly_repository_record	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that agent_foundations claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly repository record source for agent_foundations; routed to Foundations of AGEINT (agent definition, PEAS framework, rational agents); AGEINT Python Code Library. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Rao, 1995]	BDI Agents: From Theory to Practice	curriculum_anchor	agent_foundations	scholarly_repository_record	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that agent_foundations claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly repository record source for agent_foundations; routed to Foundations of AGEINT (agent architectures); Design Patterns & Archetypes (goal-directed agent archetypes). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Vaswani, 2017]	Attention Is All You Need	curriculum_anchor	llm_architecture	scholarly_preprint	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that llm_architecture claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly preprint source for llm_architecture; routed to Foundations of AGEINT (LLM substrate); LangChain/LangGra Patterns appendix; CrewAI appendix; AutoGen/MCP appendix. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Yao, 2023b]	Tree of Thoughts: Deliberate Problem Solving with LLMs	curriculum_anchor	agentic_reasoning	scholarly_preprint	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that agentic_reasoning claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly preprint source for agentic_reasoning; routed to Foundations of AGEINT (reasoning architectures); Design Patterns & Archetypes (planning patterns); LangChain/LangGra Patterns appendix. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Lewis, 2020]	Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks	curriculum_anchor	agentic_memory	scholarly_preprint	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that agentic_memory claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly preprint source for agentic_memory; routed to Foundations of AGEINT (agent memory); Design Patterns & Archetypes (RAG architecture); LangChain/LangGra Patterns appendix; AGEINT Python Code Li…. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Patil, 2023]	Gorilla: Large Language Model Connected with Massive APIs	curriculum_anchor	tool_use_agents	scholarly_preprint	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that tool_use_agents claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly preprint source for tool_use_agents; routed to Foundations of AGEINT (tool-use patterns); AGEINT Python Code Library; LangChain/LangGra Patterns appendix. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Qin, 2023]	ToolLLM: Facilitating Large Language Models to Master 16000+ Real-world APIs	curriculum_anchor	tool_use_agents	scholarly_preprint	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that tool_use_agents claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly preprint source for tool_use_agents; routed to Foundations of AGEINT (tool-use); AGEINT Python Code Library; LangChain/LangGra Patterns appendix. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Wu, 2023]	AutoGen: Enabling Next-Gen LLM Applications via Multi-Agent Conversation	curriculum_anchor	multi_agent_frameworks	scholarly_preprint	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that multi_agent_frameworks claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly preprint source for multi_agent_framew routed to AutoGen and MCP Patterns appendix; Frameworks & Infrastructure; CrewAI appendix (comparison context). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[LangChain, 2025a]	LangChain Documentation	curriculum_anchor	agentic_framework_docs	professional_documentation	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that agentic_framework_docs claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified professional documentation source for agentic_framework_docs routed to LangChain/LangGra Patterns appendix; AGEINT Python Code Library. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[LangChain, 2025b]	LangGraph Documentation	curriculum_anchor	agentic_frameworks_docs	professional_documentation	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that agentic_framework_docs claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified professional documentation source for agentic_framework_docs routed to LangChain/LangGra Patterns appendix; AGEINT Python Code Library; Frameworks & Infrastructure. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[CrewAI, 2025]	CrewAI Documentation	curriculum_anchor	agentic_frameworks_docs	professional_documentation	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that agentic_framework_docs claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified professional documentation source for agentic_framework_docs routed to CrewAI Multi-Agent appendix; Frameworks & Infrastructure. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Liang, 2022]	Holistic Evaluation of Language Models	curriculum_anchor	llm_evaluation	scholarly_preprint	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that llm_evaluation claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly preprint source for llm_evaluation; routed to Frameworks & Infrastructure (model evaluation); Security & Adversarial Considerations (model capability assessment); AGEINT Python Code Library. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Srivastava, 2022]	Beyond the Imitation Game: Quantifying and Extrapolating the Capabilities of LLMs	curriculum_anchor	llm_evaluation	scholarly_preprint	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that llm_evaluation claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly preprint source for llm_evaluation; routed to Frameworks & Infrastructure (model evaluation); Security & Adversarial Considerations; AGEINT Python Code Library. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Perez, 2022]	Ignore Previous Prompt: Attack Techniques For Language Models	curriculum_anchor	adversarial_ai_security	scholarly_preprint	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that adversarial_ai_security claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly preprint source for adversarial_ai_security; routed to Security & Adversarial Considerations; ATT&CK & Kill Chain Templates appendix; Cognitive Security & Inoculation appendix. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Ericsson, 1993]	The Role of Deliberate Practice in the Acquisition of Expert Performance	curriculum_anchor	cognitive_performance	scholarly_repository_record	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that cognitive_performance claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly repository record source for cognitive_performance; routed to Productivity Intelligence & Cognitive Performance (cognitive athlete, deliberate practice); Instructor Capstone/Rubric/Re Team Pack appendix. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Cepeda, 2006]	Distributed Practice in Verbal Recall Tasks	curriculum_anchor	cognitive_performance	scholarly_repository_record	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that cognitive_performance claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly repository record source for cognitive_performance; routed to Productivity Intelligence & Cognitive Performance (information architecture, spaced repetition); Instructor Capstone/Rubric/Re Team Pack appendix. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[Walker, 2006]	Sleep, Memory, and Plasticity	curriculum_anchor	cognitive_performance	scholarly_repository_record	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that cognitive_performance claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly repository record source for cognitive_performance; routed to Productivity Intelligence & Cognitive Performance (sleep and cognition); Cognitive Security & Inoculation appendix. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Kaplan, 1989]	The Experience of Nature: A Psychological Perspective	curriculum_anchor	cognitive_performance	scholarly_book_metadata	2026-06-16	annual	instructor, analyst, reviewer, and curriculum maintainer	Checks that cognitive_performance claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified scholarly book metadata source for cognitive_performance; routed to Productivity Intelligence & Cognitive Performance (attention restoration, information architecture); Cognitive Security & Inoculation appendix. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.
[of Standards and Technology., 2024]	NIST IR 8547: Transition to Post-Quantum Cryptography Standards	curriculum_anchor	cryptographic_standards	official_standard_draft	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that cryptographic_standards claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified official draft source for cryptographic_standards; routed to Cryptographic Methods appendix; Security & Adversarial Considerations. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

Citation key	Title	Role	Lane	Tier	Checked	Refresh	Stakeholder	Assurance use	Rights dimension	Source note
[Weng, 2023]	LLM-powered Autonomous Agents	curriculum_anchor	agentic_design_principles	professional_documentation	2026-06-16	semiannual	instructor, analyst, reviewer, and curriculum maintainer	Checks that agentic_design_principles claims stay source-backed, bounded, and separated from operational practice.	public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary	Verified professional documentation source for agentic_design_principle routed to Foundations of AGEINT (agent memory, tool use, planning); Design Patterns & Archetypes. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution.

References

Evidence anchor. Section 80.

The render pipeline reads `references-*.bib`, which is generated from parsed curriculum data plus official source-quality anchors. Manuscript prose should cite with Pandoc citation keys such as `[@ageint137]`; do not paste bibliography entries into source prose.

References

SIST Guide Reference 001. Epistemic governance in the context of crisis, 2026. URL https://journals.sagepub.com/doi/10.1177/00953997241303935. This article examines the concept of epistemic governance during crises.

SIST Guide Reference 002. Objectivity, 2026. URL https://www.dni.gov/index.php/how-we-work/objectivity. ICD 203 directs the heads of IC elements to designate a similar individual or office to respond.

SIST Guide Reference 003. Active inference: Applicability to different types of social, 2026. URL https://pmc.ncbi.nlm.nih.gov/articles/PMC7916013/. A 2021 peer-reviewed article by Stephen Fox in the journal Entropy that relates the active inference framework to social organization. It maps concepts such as variational free energy, prediction error, generative models, and Markov blankets onto industrial engineering and quality management practices, treating organizational survival as the maintenance of process control limits.

SIST Guide Reference 004. Ai won't replace spies-it will make them more powerful than ever, 2026. URL https://fedgovtoday.com/podcast/ai-wont-replace-spies-it-will-make-them-more-powerful-than-ever. Tom Mulligan argues that artificial intelligence will enhance rather than replace human intelligence professionals, contending that the future of intelligence lies in human-machine collaboration. He maintains that uniquely human qualities such as intuition, experience, and independent judgment become more valuable as adversaries gain access to the same AI tools.

SIST Guide Reference 005. Cia: Studies in ai and human intelligence - semperverus, 2026. URL https://www.semperverus.com/cia-studies-in-ai-and-human-intelligence/. A blog post on SemperVerus summarizing a CIA Studies in Intelligence article, "Espionage in Our AI Future: Why Human Intelligence Still Matters" (Vol. 70, No. 1, March 2026). It argues that as AI makes technical intelligence cheaper and AI-driven fabrication more pervasive, human intelligence becomes relatively more valuable, since human specialists are needed to verify source reliability over time.

SIST Guide Reference 006. Director of national intelligence - intelligence community directives, 2026. URL https://irp.fas.org/dni/icd/index.html. A Federation of American Scientists repository cataloguing the Intelligence Community Directives (ICDs) issued by the Director of National Intelligence. ICDs are the principal means by which the DNI provides policy, guidance, and direction to the U.S. Intelligence Community.

SIST Guide Reference 007. The friends britain's post-war secret intelligence, 2026. URL https://www.cia.gov/readingroom/document/cia-rdp96b01172r000100060001-5. It is SIS's task to pursue policy objectives by unorthodox means and to amass useful information.

SIST Guide Reference 008. Mossad | military history and science, 2026. URL https://www.ebsco.com/research-starters/military-history-and-science/mossad. An EBSCO Research Starter reference article on the Mossad, Israel's national intelligence agency established in 1949 and responsible for foreign intelligence collection and counterterrorism operations conducted outside Israel's borders. It describes the agency's departmental structure (collection, political action and liaison, research, technology) and reviews historically documented operations including the 1960 capture of Adolf Eichmann and the rescue of Ethiopian Jews.

SIST Guide Reference 009. "here to stay" - chinese state-affiliated hacking for strategic goals, 2026. URL https://merics.org/en/report/here-stay-chinese-state-affiliated-hacking-strategic-goals. A November 2023 report from MERICS (Mercator Institute for China Studies) analyzing Chinese state-affiliated cyber intrusions aimed at strategic goals. It argues that Chinese actors pursue long-term, persistent access to European technology firms and critical infrastructure for espionage rather than disruption, with targeting aligned to government priorities such as semiconductors, pharmaceuticals, and advanced manufacturing.

SIST Guide Reference 010. The five eyes archive, 2026. URL https://unredacted.uk/project-archives/five-eyes/. An online archive maintained by Unredacted UK that compiles declassified government documents on intelligence sharing among the Five Eyes nations (United States, United Kingdom, Canada, Australia, and New Zealand). The collection traces the emergence and evolution of bilateral and multilateral agreements from the postwar era, including the BRUSA and UKUSA agreements, drawing on records from UK, US, and Australian agencies plus freedom-of-information releases.

SIST Guide Reference 011. Brusa and ukusa agreements: Gchq and nsa, 2026. URL https://unredacted.uk/collections/ukusa-2010/. A curated collection from Unredacted UK presenting documents declassified by the NSA and GCHQ in 2010 relating to US-UK signals intelligence cooperation. It covers the 1946 British-US Communications Agreement (BRUSA), its wartime origins from 1940, and its evolution into the 1956 UKUSA Agreement and the broader Five Eyes alliance.

SIST Guide Reference 012. Counterintelligence activities of non-state actors - grey dynamics, 2026. URL https://greydynamics.com/counterintelligence-activities-of-non-state-actors/. A Grey Dynamics analysis article (Rachel Brown, 2021) on how non-state actors conduct counterintelligence. It argues that although such groups lack the technical collection capabilities of states, they compensate through open-source and human-source methods and benefit defensively from compartmentalized, cell-based structures and ideological cohesion.

SIST Guide Reference 013. Intelligence tradecraft overview | pdf | surveillance, 2026. URL https://www.scribd.com/presentation/580627740/Lesson-8-Introduction-to-Intelligence-Tradecraft. This is an instructional training document hosted on Scribd that introduces the fundamentals of intelligence tradecraft, defined as the methods and skills used in intelligence operations. It covers core concepts and types of tradecraft, cover and operational security, casing and surveillance, clandestine communication, and information gathering.

SIST Guide Reference 014. Tradecraft: Covert operative tactics and techniques, 2026. URL https://trdcrft.com/tradecraft-covert-operative-tactics-and-techniques/. An educational article from TRDCRFT defining tradecraft as the techniques, strategies, and tools used by intelligence operatives to pursue objectives while maintaining secrecy and operational security. It surveys core disciplines such as surveillance and counter-surveillance, cover and disguise, technical and human intelligence work, and the field's evolution toward digital and cyber methods.

SIST Guide Reference 015. Cover (intelligence gathering), 2026. URL https://en.wikipedia.org/wiki/Cover_(intelligence_gathering). A Wikipedia article explaining the concept of cover in human intelligence and counterintelligence work, defined as the ostensible identity assumed by a covert agent. It distinguishes official cover (diplomatic channels, immunity) from non-official cover (no government acknowledgment, less protection). The article surveys historical examples of front organizations and assumed identities.

SIST Guide Reference 016. Surveillance detection - state.gov, 2026. URL https://2009-2017.state.gov/documents/organization/209870.pdf. Place where victim can be controlled with limited avenues of escape.

SIST Guide Reference 017. Language of espionage | international spy museum, 2026. URL https://www.spymuseum.org/education-programs/spy-resources/language-of-espionage/. An educational glossary from the International Spy Museum, a nonprofit institution in Washington, DC, presenting an alphabetized dictionary of espionage terminology. It defines operational roles (agent, handler, case officer), intelligence disciplines such as HUMINT, SIGINT, and IMINT, major organizations (CIA, FBI, KGB, MI5, MI6, NSA), and historical equipment like the Enigma machine and U-2 aircraft.

SIST Guide Reference 018. Old-school spycraft could make a comeback as ai undermines trust, 2026. URL https://www.nextgov.com/artificial-intelligence/2026/04/old-school-spycraft-could-make-comeback-ai-undermines-trust/412532/. A Nextgov article reporting on an essay in the CIA's Studies in Intelligence journal by RAND researcher Thomas Mulligan. It argues that as AI makes deepfakes and synthetic communications easier, trust in digital channels erodes, paradoxically increasing the value of traditional human intelligence methods.

SIST Guide Reference 019. Espionage in our ai future: Why human intelligence still matters - csi, 2026. URL https://www.cia.gov/resources/csi/studies-in-intelligence/studies-in-intelligence-vol-70-no-1-extracts-march-2026/espionage-in-our-ai-future-why-human-intelligence-still-matters/. By Thomas Mulligan, a researcher at the RAND Corporation who served in CIA during 2008-14.

SIST Guide Reference 020. The human source management system (confidential informant, 2026. URL https://www.hsmtraining.com/human-source-management-system-book. A publisher and training-organization page from HSM Training and Consultancy (London) promoting the book The Human Source Management System, a guide of over 500 pages that applies social psychology to the management of confidential informants. The site states the book draws on research and practitioner interviews and is used by law enforcement and intelligence bodies across more than 40 countries.

SIST Guide Reference 021. Learn how to be a spy from previously unpublished kgb training, 2026. URL https://theworld.org/stories/2019/07/26/learn-how-be-spy-literally. A July 2019 story from The World (PRX public radio) about a project led by Michael Weiss to translate previously unpublished Soviet-era KGB training manuals from the 1970s-80s into English. The article describes how the manuals cover intelligence methods such as agent recruitment, psychological manipulation, and disinformation detection, and notes the materials remain relevant because related methods persist in modern Russian services.

SIST Guide Reference 022. Summaries of newly obtained kgb training manuals - the interpreter, 2026. URL https://www.interpretermag.com/new-kgb-manuals/. An article from The Interpreter, a publication focused on Russian affairs and disinformation, announcing a project to translate, analyze, and publish previously unpublished Soviet KGB training documents. It summarizes a set of newly obtained manuals spanning several decades and describes the topics they cover, including operational terminology, agent classification, information-gathering methods, recruitment and vetting procedures, and counterintelligence concerns.

SIST Guide Reference 023. The impact of digital technology on clandestine agent recruitment, 2026. URL https://dspace.cuni.cz/bitstream/handle/20.500.11956/197697/120483459.pdf?sequence=1&isAllowed=y. A 2024 International Master in Security, Intelligence and Strategic Studies thesis (Glasgow, Trento, Charles University) titled 'Human Intelligence in the Modern Era: The Impact of Digital Technology on Clandestine Agent Recruitment.' It uses a literature-based analysis plus three case studies to compare traditional human-source practices with technology-enabled approaches.

SIST Guide Reference 024. Using shared experiences to recruit committed human intelligence, 2026. URL https://bpspsychub.onlinelibrary.wiley.com/doi/10.1111/lcrp.12251. SIST guide bibliography entry.

SIST Guide Reference 025. Andrew bustamante: Inside the mind of a spy - tradecraft, trust, 2026. URL https://shows.acast.com/the-unmistakable-creative-podcast/episodes/andrew-bustamante-v2. This is an episode of The Unmistakable Creative Podcast featuring former CIA field operative Andrew Bustamante discussing intelligence work. The conversation covers his background at the Air Force Academy and CIA training, and frames espionage as resting on reading people, trust, influence, and empathy rather than glamour or action. It also addresses how operatives are selected, the isolation of covert work, and its psychological effects on personal relationships.

SIST Guide Reference 026. The tension and drama behind surveillance detection operations, 2026. URL https://www.youtube.com/watch?v=duymZEwvxL8. A YouTube video titled "Inside the CIA: The tension and drama behind surveillance detection operations," released May 3, 2024, featuring a former CIA officer. The speaker describes the operational complexity and interpersonal tension involved in moving safely from a starting point to a meeting while accounting for the presence of hostile observation. It conveys the difficulty and stress of clandestine field meetings as recounted from personal experience.

SIST Guide Reference 027. The dead drop: Design a communications method like a spy, 2026. URL https://www.youtube.com/watch?v=CRhGs3b27SA. Learn a technique for communicating with your family in an emergency using a method used by spies.

SIST Guide Reference 028. Introducing dead drops to network steganography using arp-caches and snmp-walks, 2026. URL https://dl.acm.org/doi/10.1145/3339252.3341488. SIST guide bibliography entry.

SIST Guide Reference 029. Agent handling in counterintelligence | pdf, 2026. URL https://www.scribd.com/document/513316188/Intelligence-Agenthandling. A roughly 28-page Scribd document titled "Agent Handling in Counterintelligence" providing an educational overview of intelligence operations. It surveys the roles of case officers in managing sources, recruitment and training of agents, protective measures such as fronts and cutouts, agent classifications including unwitting sources, and counterintelligence methods for identifying foreign operatives and reducing security breaches.

SIST Guide Reference 030. The secrets of countersurveillance, 2026. URL https://telluric.us/the-secrets-of-countersurveillance/. SIST guide bibliography entry.

SIST Guide Reference 031. Kgb counter surveillance: How to know if you're being followed, 2026. URL https://www.reddit.com/r/TheAmericans/comments/1cmnia2/kgb_counter_surveillance_how_to_know_if_youre/. There are cameras everywhere! Everything is trackable!

SIST Guide Reference 032. Top secret kgb training manual - working with agents, 2026. URL https://books.google.com/books/about/TOP_SECRET_KGB_Training_Manual_Working_w.html?id=rM540QEACAAJ. A Google Books catalog entry for a 2025 English-translation edition of a Cold War-era Soviet intelligence training manual, published by Century Print Media Group with a translator's note by a retired NATO intelligence officer. The 144-page volume is presented as a historical document on Soviet human-intelligence doctrine and counterintelligence practice.

SIST Guide Reference 033. The counterintelligence threat from non-state actors, 2026. URL https://www.tandfonline.com/doi/pdf/10.1080/08850600802698200. How seriously is the U.S. Intelligence Community (IC) considering this challenge to U.S.

SIST Guide Reference 034. Studies in intelligence vol. 70, no. 1 (extracts, march 2026) - csi, 2026. URL https://www.cia.gov/resources/csi/studies-in-intelligence/studies-in-intelligence-vol-70-no-1-extracts-march-2026/. Thomas Mulligan is a researcher at the RAND Corporation and former CIA officer. Ana P.

SIST Guide Reference 035. Signals intelligence (sigint) overview, 2026. URL https://www.nsa.gov/Signals-Intelligence/Overview/. SIGINT is intelligence derived from electronic signals and systems used by foreign targets.

SIST Guide Reference 036. European axis signal intelligence in world war ii, 2026. URL https://www.nsa.gov/Helpful-Links/NSA-FOIA/Declassification-Transparency-Initiatives/Historical-Releases/European-Axis-SIGINT/. Volumes 1 - 9 of the European Axis Signal Intelligence in WWII documentation.

SIST Guide Reference 037. Nsa releases history of american sigint and the vietnam war, 2026. URL https://fas.org/publication/nsa_releases_history_of_americ/. This Federation of American Scientists article reports on the NSA's declassification of a roughly 500-page historical study titled "Spartans in Darkness," which examines American signals intelligence during the Vietnam War from 1945 to 1975. Author Robert J. Hanyok documents that no second attack occurred during the 1964 Gulf of Tonkin Incident, contradicting prior official testimony, and also covers episodes such as the Tet Offensive and the Son Tay prison rescue.

SIST Guide Reference 038. History of signals intelligence at the cia - open int, 2026. URL https://open-int.blog/2018/01/15/history-of-signals-intelligence-at-the-cia/. A January 2018 blog post on Open INT recounting the CIA's role in signals intelligence from roughly 1947 to 1970,

noting that SIGINT is often associated with the NSA but the CIA also participated. It distinguishes communications intelligence from electronic intelligence and references declassified Cold War operations including U-2 collection and a Berlin communications-tapping effort.

SIST Guide Reference 039. The cia and signals intelligence | national security archive, 2026. URL https://nsarchive.gwu.edu/briefing-book/cyber-vault-intelligence/2015-03-20/cia-and-signals-intelligence. A 2015 briefing book from the National Security Archive, compiled by Jeffrey T. Richelson, presenting declassified documents on the CIA's signals intelligence activities from roughly 1947 to 1970. It documents the CIA's parallel SIGINT operations alongside the NSA during the Cold War, covering programs and collection efforts as well as recurring friction between the two agencies over mission overlap, budgets, and access to intelligence.

SIST Guide Reference 040. Basic cryptography, 2026. URL https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/friedman-documents/publications/FOLDER_238/41748889078809.pdf. Codes will first be considered, but as they do not fulfill the conditions required of a means.

SIST Guide Reference 041. Five eyes foia disclosures, 2026. URL https://unredacted.uk/collections/five-eyes-us-foia/. A collection page from Unredacted, a UK-based organization focused on declassified government records. It assembles over 70 documents obtained through a 2017 Freedom of Information Act legal challenge led by Privacy International, drawn from US agencies including the NSA, State Department, and Department of Defense.

SIST Guide Reference 042. Five eyes foia disclosures: key documents, 2026. URL https://unredacted.uk/briefings/five-eyes-foia-key-documents/. A briefing from Unredacted examining previously classified Five Eyes documents released to Privacy International following a 2017 US freedom of information request. The materials, spanning 1945 to 2016, trace the development and functioning of the UKUSA Agreement underpinning intelligence cooperation among the US, UK, Canada, Australia, and New Zealand.

SIST Guide Reference 043. Technical surveillance countermeasures (tscm) - bastille networks, 2026. URL https://bastille.net/centers-of-excellence/tscm/. An informational guide from Bastille Networks explaining Technical Surveillance Countermeasures (TSCM), defined as security measures aimed at detecting and neutralizing surveillance devices to protect sensitive communications. It traces TSCM origins to World War II and Cold War intelligence work and catalogues threat types such as radio-frequency transmitters, hidden cameras, and acoustic eavesdropping.

SIST Guide Reference 044. Technical surveillance threat levels - granite island group, 2026. URL http://www.tscm.com/threatlvls.html. A reference page from the Granite Island Group describing a ten-level taxonomy of technical surveillance threats and the corresponding technical surveillance countermeasures (TSCM) inspections used to detect them. It explains that detection difficulty increases by roughly an order of magnitude at each level, grouping threats into clusters and beginning with low-power consumer-grade devices.

SIST Guide Reference 045. Tscm | technical surveillance countermeasures - pinkerton, 2026. URL https://pinkerton.com/investigations/tscm-technical-surveillance-countermeasures. A service page from Pinkerton describing technical surveillance countermeasures used to detect and prevent corporate eavesdropping and protect intellectual property. It outlines examination methods including infrared spectrum analysis to find heat signatures of hidden devices, radio frequency analysis to identify wireless audio bugs, and physical inspection for tampered equipment or poor security practices.

SIST Guide Reference 046. The tscm inspection process | by murray associates tscm, 2026. URL https://counterespionage.com/tscm-inspection-process/. A web page from Murray Associates, a counterespionage consulting firm, explaining the technical surveillance countermeasures (TSCM) inspection process used to detect eavesdropping and surveillance devices in buildings. It outlines a three-phase methodology: a pre-inspection planning discussion, an on-site evaluation combining visual examination, technical instrumentation, and information-security review, and a post-inspection written report with findings and recommendations.

SIST Guide Reference 047. How the intelligence community has held back open-source, 2026. URL https://www.cia.gov/resources/csi/studies-in-intelligence/studies-in-intelligence-68-no-2-june-2024/commentary-how-the-intelligence-community-has-held-back-open-source-intelligence-and-how-it-needs-to-change/. Plans and strategies for improving open-source intelligence (OSINT) operations in the Intelligence.

SIST Guide Reference 048. The ic osint strategy 2024-2026, 2026. URL https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf. Tradecraft and training standards must be flexible and updated regularly to keep pace with changes.

SIST Guide Reference 049. Open source intelligence (osint): issues and trends, 2026. URL https://www.academia.edu/69776570/Open_Source_Intelligence_OSINT_issues_and_trends. The text explores OSINT's advantages and disadvantages in intelligence activities.

SIST Guide Reference 050. Thoughts on bazzell's new book? [open source intelligence, 2026. URL https://www.reddit.com/r/OSINT/comments/egnki0/thoughts_on_bazzells_new_book_open_source/. Mike wrote he wants to make the OSINT investigator more self reliant, able to do his job without.

SIST Guide Reference 051. Chapter 5: From recon-ng to trace labs - a tour of the best open, 2026. URL https://subscription.packtpub.com/book/security/9781837638277/5/ch05lvl1sec37/additional-open-source-osint-tools. SIST guide bibliography entry.

SIST Guide Reference 052. What is open source intelligence & top 10 tools - lampyre, 2026. URL https://lampyre.io/blog/what-is-open-source-intelligence-top-10-tools/. This article defines open source intelligence as the practice of gathering information from publicly available data for security, business, and investigative purposes, drawing on websites, social media, government records, and public databases.

SIST Guide Reference 053. A guide to choosing the right tool for your needs, 2026. URL https://www.linkedin.com/pulse/guide-choosing-right-tool-your-needs-lijin-thomas-abraham-pmp. SIST guide bibliography entry.

SIST Guide Reference 054. What are your preferred osint tools? : r/hacking, 2026. URL https://www.reddit.com/r/hacking/comments/vr7bah/what_are_your_preferred_osint_tools/. Recommended OSINT tools and their benefits. Top open source intelligence websites.

SIST Guide Reference 055. Inteltechniques books, 2026. URL https://inteltechniques.com/book1.html. OSINT Techniques. Resources for Uncovering Online Information - 11th Edition (2024).

SIST Guide Reference 056. Inteltechniques - osint 11 2025.04.02 .pdf - elhacker.info, 2026. URL https://elhacker.info/manuales/Hacking%20y%20Seguridad%20informatica/IntelTechniques%20-%20OSINT%2011%202025.04.02%20.pdf. All tutorials in this book were confirmed accurate as of November 1, 2024.

SIST Guide Reference 057. Mcrp 2-10b.4 (secured) - marines.mil, 2026. URL https://www.marines.mil/Portals/1/Publications/MCRP%202-10B.4%20(SECURED).pdf?ver=AA0e4-I3dfLOoR02nnMbZw%3D%3D. MCRP 2-10B.4 in the source guide links to the Marines GEOINT manual, not a reconnaissance manual. The linked PDF is 'Geospatial Intelligence Support to Operations'; verify the intended citation before reuse.

SIST Guide Reference 058. Geoint essential body of knowledge, 2026. URL https://usgif.org/wp-content/uploads/2020/11/ebk2019.pdf. The GEOINT Essential Body of Knowledge (Version 2.0, 2019), published by the United States Geospatial Intelligence Foundation (USGIF). First developed in 2014 and revised with community input, it defines the competencies, standards, and learning objectives needed to succeed in the geospatial intelligence discipline.

SIST Guide Reference 059. neonpangolin/geospatial-intelligence-library, 2026. URL https://github.com/neonpangolin/geospatial-intelligence-library. A GitHub repository describing itself as a reference toolkit for geolocation and chronolocation in digital investigations. It curates open-source resources organized into categories including satellite imagery, mapping, infrastructure and transport tracking, weather and environmental monitoring, shadow and sun-position tools for time-of-day analysis, crisis and conflict mapping, image forensics, and geocoding utilities.

SIST Guide Reference 060. Dodm 3305.10, "dod geospatial intelligence (geoint, 2026. URL https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/330510m.pdf?ver=2019-08-20-104118-973. SIST guide bibliography entry.

SIST Guide Reference 061. Cyber kill chain(r), 2026. URL https://web.archive.org/web/20201228171034/https:/www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. This Lockheed Martin webpage describes the Cyber Kill Chain framework, a methodology for identifying and preventing cyber intrusions as part of the company's Intelligence Driven Defense model. It outlines the sequence of steps an adversary must complete to achieve an objective, and is intended to help analysts understand attacker tactics and procedures.

SIST Guide Reference 062. Cyber kill chain, 2026. URL https://en.wikipedia.org/wiki/Cyber_kill_chain. A Wikipedia article describing the cyber kill chain, a framework adapted by Lockheed Martin from a military concept to model how cyberattacks progress through distinct phases. It outlines seven stages from reconnaissance through actions on objectives, along with defensive countermeasures organizations can apply at each stage.

SIST Guide Reference 063. Enterprise matrix - mitre att&ck(r), 2026. URL https://attack.mitre.org/matrices/enterprise/. The official MITRE ATT&CK Enterprise Matrix, a curated knowledge base of adversary tactics and techniques observed in real-world intrusions. It organizes activity into fifteen sequential tactics, from reconnaissance and resource development through initial access, persistence, privilege escalation, defense evasion, credential access, lateral movement, command and control, exfiltration, and impact.

SIST Guide Reference 064. Mitre att&ck(r), 2026. URL https://attack.mitre.org. MITRE ATT&CK is a globally accessible knowledge base that catalogs adversary tactics and techniques drawn from real-world observations of cyber intrusions. The framework is organized into matrices covering Enterprise, Mobile, and Industrial Control Systems environments, with tactics representing adversary objectives and techniques describing specific methods used to achieve them.

SIST Guide Reference 065. Enterprise techniques - mitre att&ck(r), 2026. URL https://attack.mitre.org/techniques/enterprise/. The Enterprise Techniques page of the MITRE ATT&CK framework, a cybersecurity knowledge base maintained by MITRE Corporation. It documents 222 enterprise techniques and 475 sub-techniques describing how adversaries achieve tactical goals across the attack lifecycle, organized by tactics such as initial access, persistence, privilege escalation, defense evasion, credential access, discovery, and impact.

SIST Guide Reference 066. What is stix/taxii? - cloudflare, 2026. URL https://www.cloudflare.com/learning/security/what-is-stix-and-taxii/. A Cloudflare Learning Center explainer describing STIX and TAXII as complementary standards for cyber threat intelligence. STIX defines a structured language for representing threat information, while TAXII specifies how that information is transported and exchanged between systems. Together they form a framework that lets organizations share and consume threat intelligence in a consistent, machine-readable way to improve collective defense.

SIST Guide Reference 067. Introduction to stix, 2026. URL https://oasis-open.github.io/cti-documentation/stix/intro.html. An introductory page from the OASIS CTI documentation explaining STIX (Structured Threat Information Expression), an open-source language and serialization format used to exchange cyber threat intelligence. It describes how STIX 2.1 models intelligence using 18 domain objects (such as attack patterns, malware, threat actors, and vulnerabilities) and 2 relationship objects, all represented as JSON.

SIST Guide Reference 068. Oasis cyber threat intelligence (cti) tc, 2026. URL https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti. The official committee page for the OASIS Cyber Threat Intelligence (CTI) Technical Committee, a standards body that develops formats for sharing cyber threat intelligence. It maintains the STIX (Structured Threat Information Expression) data model and the TAXII exchange protocol, both approved as OASIS standards in 2021, and organizes subcommittees for STIX, TAXII, and interoperability.

SIST Guide Reference 069. Assessing nation-state-sponsored cyberattacks using aspects, 2026. URL https://onlinelibrary.wiley.com/doi/10.1111/1745-9133.12646. They found that the most common cyberattacks initiated by nation-states were espionage focused.

SIST Guide Reference 070. Getting harder to catch analyzing the evolution of china's cyber, 2026. URL https://www.cs.tufts.edu/comp/116/archive/fall2016/wdesombre.pdf. A 2016 student security paper by Winnona DeSombre (Tufts Comp116) analyzing the evolution of China's cyber espionage campaigns against the United States. Organized in three parts, it surveys China-US relations in the cyber domain and the policy dilemmas of attribution and shared terminology, presents a case study of the APT1 hacker group linked to PLA Unit 61398, and reviews broader trends in the context of the 2015 US-China Cyber Agreement.

SIST Guide Reference 071. I led ir on nation-state attacks at mandiant, fireeye & crowdstrike, 2026. URL https://www.reddit.com/r/cybersecurity/comments/1q3k69c/ama_interest_check_i_led_ir_on_nationstate/. Attribution becomes harder when its open-source.

SIST Guide Reference 072. Att&ck-based advanced persistent threat attacks risk propagation, 2026. URL https://www.sciencedirect.com/science/article/abs/pii/S1389128624002081. The Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework introduced.

SIST Guide Reference 073. Solarwinds supply chain attack - fortinet, 2026. URL https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack. This Fortinet cybersecurity glossary page provides educational material about the SolarWinds supply chain attack. It explains how attackers compromised SolarWinds' Orion monitoring software with malicious code that spread to roughly 18,000 customers through software updates beginning in early 2020, and notes the attack's extended timeline and impact on U.S. federal agencies and major companies.

SIST Guide Reference 074. How to protect against a supply chain compromise - vectra ai, 2026. URL https://www.vectra.ai/blog/takeaways-from-the-xz-utils-backdoor. A Vectra AI blog post from April 2024 analyzing the XZ Utils backdoor, a malicious commit discovered on March 29, 2024 in a widely used open-source compression library that could compromise affected systems via SSH. The article frames the incident as a supply chain compromise affecting both open-source and commercial software, drawing comparison to SolarWinds.

SIST Guide Reference 075. The xz-utils backdoor: The supply chain rce that got caught, 2026. URL https://www.invicti.com/blog/web-security/xz-utils-backdoor-supply-chain-rce-that-got-caught. An Invicti Security blog post from April 2024 analyzing the xz-utils backdoor, a software supply chain compromise discovered in versions 5.6.0 and 5.6.1 of the compression library. It describes how malicious code was hidden in test files and assembled only during compilation, potentially enabling unauthenticated remote code execution via OpenSSH, and how a long-term contributor gradually gained maintainer trust before inserting it.

SIST Guide Reference 076. Xz utils backdoor, 2026. URL https://en.wikipedia.org/wiki/XZ_Utils_backdoor. In early 2024, a malicious backdoor was discovered embedded in XZ Utils, a widely used compression library in Linux distributions, designed to enable unauthorized remote code execution via OpenSSH using an Ed448 private key. The perpetrator, operating under the pseudonym Jia Tan, spent over two years building trust as a contributor before inserting the exploit, which received a maximum CVSS score of 10.0.

SIST Guide Reference 077. An evidence-driven analysis of threat information sharing, 2026. URL https://arxiv.org/html/2512.18714v3. An arXiv research paper presenting an evidence-driven analysis of why threat information sharing for industrial control systems remains ineffective. Drawing

on three major ICS attacks and a review of 196 procedure examples across 22 malware families, it identifies limitations including incomplete support in the STIX sharing standard, reliance on proprietary undocumented protocols, and insufficient technical detail in threat and vulnerability reports.

SIST Guide Reference 078. Advanced criminal investigations and intelligence operations: Tradecraft methods, practices, tactics, and techniques|paperback, 2026. URL https://www.barnesandnoble.com/w/advanced-criminal-investigations-and-intelligence-operations-robert-j-girod/1117653651. A Barnes & Noble listing for Advanced Criminal Investigations and Intelligence Operations by Robert J. Girod. The book examines tradecraft, defined as the methods, practices, and techniques used in espionage and clandestine investigations.

SIST Guide Reference 079. Financial intelligence, 2026. URL https://en.wikipedia.org/wiki/FININT. The Wikipedia article on financial intelligence (FININT), defined as gathering information about the financial affairs of entities of interest to understand their nature, capabilities, and intentions. It outlines two core components: collection, in which Financial Intelligence Units gather transaction data and suspicious activity reports from banks, and analysis, in which specialists use data mining to detect tax evasion, money laundering, and terrorist financing.

SIST Guide Reference 080. Financial intelligence, 2026. URL https://en.wikipedia.org/wiki/Financial_intelligence. A Wikipedia article on financial intelligence (FININT), the gathering and analysis of information about financial transactions to detect illicit activity such as money laundering, tax evasion, and terrorist financing. It distinguishes two core functions: collection of raw transaction data and suspicious activity reports by government financial intelligence units, and analysis using data-matching techniques to identify suspicious patterns. The article describes the U.S.

SIST Guide Reference 081. Financial intelligence, 2026. URL https://en.citizendium.org/wiki/Financial_intelligence. The Citizendium 'Financial intelligence' article was never written; the page is empty. Use an authoritative alternative source for financial intelligence definitions.

SIST Guide Reference 082. Financial intelligence: A crucial pillar of national security, 2026. URL https://www.scirp.org/pdf/me_7204164.pdf. A 2025 article by Kevin Hk Chow in Modern Economy titled "Financial Intelligence: A Crucial Pillar of National Security." It argues that Financial Intelligence (FININT) serves as a critical interface between economic systems and national security, used to detect and disrupt illicit financial networks tied to money laundering, terrorism financing, and transnational crime.

SIST Guide Reference 083. Jp 3-53, "doctrine for joint psychological operations", 2026. URL https://nsarchive2.gwu.edu/NSAEBB/NSAEBB177/02_psyop-jp-3-53.pdf. Joint Publication 3-53, the US Department of Defense joint doctrine for psychological operations. It establishes organizational structure, command relationships, planning processes, and approval authorities for integrating psychological operations into joint military campaigns and peacetime activities.

SIST Guide Reference 084. Jp 3-53 doctrine for joint psychological operations, 2026. URL http://www.bits.de/NRANEU/others/jp-doctrine/jp3_53(96).pdf. Joint Publication 3-53, Doctrine for Joint Psychological Operations (Joint Chiefs of Staff, 10 July 1996). This US military doctrine document establishes the doctrinal basis for planning and conducting psychological operations in support of joint military operations.

SIST Guide Reference 085. Military information support operations, 2026. URL https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Joint_Staff/Military_Information_Support_Operations.pdf. It sets forth joint doctrine to govern the activities and performance of the Armed Forces.

SIST Guide Reference 086. Tactical psychological operations manual | pdf | computers, 2026. URL https://www.scribd.com/doc/127025030/FM-3-05-302-Tactical-Psychological-Operations-Tactics-Techniques-And-Procedures. A U.S. military field manual, FM 3-05.302, providing doctrine for tactical psychological operations at the unit level. The roughly 255-page document covers the organization of these units, command relationships when supporting joint forces, a multi-phase product development and assessment process, and how intelligence supports such operations. It serves as a comprehensive training and reference document for personnel involved in tactical influence operations.

SIST Guide Reference 087. Fm 3-05.301 psychological operations process tactics, techniques, 2026. URL https://info.publicintelligence.net/USArmy-PsyOpsTactics.pdf.

SIST Guide Reference 088. Soviet 'active measures' forgery, disinformation, political operations, 2026. URL https://www.cia.gov/readingroom/document/cia-rdp84b00049r001303150031-0. A U.S. Department of State Bureau of Public Affairs report from October 1981, released under FOIA. It catalogs Soviet 'active measures' - the Soviet term for covert influence operations - including written disinformation, control of foreign media, use of front organizations, clandestine broadcasting, blackmail, and political influence operations. Specific cases include Soviet forgeries related to the 1979 Grand Mosque seizure and NATO theater nuclear force debates.

SIST Guide Reference 089. Soviet active measures and disinformation: Overview and assessment, 2026. URL https://www.cia.gov/readingroom/document/cia-rdp91-00901r000600200001-2. An article by Dennis Kux published in Parameters: Journal of the US Army War College (1985) and preserved in the CIA CREST archive. It defines and distinguishes Soviet 'disinformation' and 'active measures,' situating them within a spectrum of white, gray, and black foreign influence operations. Kux examines KGB front groups, agents of influence, forgeries, and the broader strategic goal of tarnishing Western governments while advancing Soviet foreign policy.

SIST Guide Reference 090. "soviet active measures: Forgery, disinformation, political operations", 2026. URL https://www.cia.gov/readingroom/document/cia-rdp84b00274r000100040004-8. A CIA CREST record (October 1981, released March 2007) comprising a routing and record sheet from the PCS/PGLO office dated February 8, 1982, attached to the same Department of State Special Report No. 88 on Soviet active measures. The document is catalogued as an open-source CREST entry and captures the internal CIA circulation of the State Department's public report on Soviet forgery and disinformation operations.

SIST Guide Reference 091. Soviet active measures and disinformation, 2026. URL https://www.cia.gov/readingroom/document/cia-rdp89g00720r000500060008-2. A declassified-in-part 1986 CIA speech text on Soviet active measures, prepared by the Foreign Activities Branch, Third World Activities Division, Office of Soviet Analysis. It explains the KGB's use of forgeries, disinformation, and front organizations to covertly influence foreign governments and publics, illustrating with the forged 1984 Olympic KKK leaflet operation designed to discourage participation in the Los Angeles Games.

SIST Guide Reference 092. Introduction, 2026. URL https://crestresearch.ac.uk/download/2409/19-025-01.pdf. A March 2019 CREST (Centre for Research and Evidence on Security Threats) report titled "Russia and Disinformation: Maskirovka," prepared by scholars of Russian foreign and security policy using open-source and Russian-language primary material. It examines the historical background of Soviet and Russian disinformation, including the concept of active measures, and how disinformation is woven into strategic narratives and diplomacy.

SIST Guide Reference 093. Deception, disinformation, and strategic communications, 2026. URL https://cs.brown.edu/people/jsavage/Deterrence/2012_NDU_ActiveMeasuresWorkingGroup.pdf. Fletcher Schoen and Christopher J. Lamb, 'Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference,' INSS Strategic Perspectives No. 11 (NDU Press, June 2012). The study examines the U.S. Active Measures Working Group, a small interagency committee formed in the 1980s to expose and counter Soviet disinformation, and analyzes why it succeeded where most such groups fail.

SIST Guide Reference 094. Deception, disinformation, and strategic communications: How one interagency group made a major difference, 2026. URL https://digitalcommons.ndu.edu/cgi/viewcontent.cgi?article=1031&context=inss-strategic-perspectives. Fletcher Schoen and Christopher J. Lamb,

'Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference,' INSS Strategic Perspectives No. 11 (NDU Press, June 2012).

SIST Guide Reference 095. Cognitive security in the age of ai, 2026. URL https://www.academia.edu/144939778/COGNITIVE_SECURITY_IN_THE_AGE_OF_AI. This policy paper examines the emergence of cognitive security.

SIST Guide Reference 096. Ai development should prioritize cognitive security, 2026. URL https://openreview.net/pdf?id=5pShDP8LSm. A position paper (Stanford authors, ICLR 2026 workshop) arguing that AI research and development should prioritize cognitive security, defined as protecting human cognitive processes from hazardous influence. It notes that generative AI systems increasingly designed to influence beliefs and behavior raise acute governance concerns, while research on these effects remains fragmented.

SIST Guide Reference 097. The history of social engineering, 2026. URL https://www.mitnicksecurity.com/the-history-of-social-engineering. This Mitnick Security guide traces the history and evolution of social engineering from antiquity through modern cyberattacks. It surveys major attack categories including phishing and its variants, pretexting, baiting, tailgating, and quid pro quo schemes, and explains the psychological influence principles such as reciprocity, scarcity, authority, and consensus that attackers exploit.

SIST Guide Reference 098. Social engineering: T he science of human hacking, 2026. URL https://theswissbay.ch/pdf/Books/Computer%20science/socialengineering_thescienceofhumanhacking_2ndedition.pdf. The full text of "Social Engineering: The Science of Human Hacking" (2nd edition, 2018) by Christopher Hadnagy, published by John Wiley & Sons. The book examines the human element of security, analyzing how manipulation and persuasion techniques can be used to influence people, and how individuals and organizations can recognize and defend against such tactics. It is written as a professional reference on understanding and countering human-targeted security threats.

SIST Guide Reference 099. Social engineering: The art of human hacking, 2026. URL https://ia801200.us.archive.org/33/items/TheAgeOfManipulationWilsonBryanKey/Social%20Engineering%20-%20the%20Art%20of%20Human%20Hacking.pdf. A PDF of the book Social Engineering: The Art of Human Hacking by Christopher Hadnagy, a foundational security text on how attackers exploit human psychology rather than technical flaws to obtain information or access. The work surveys manipulation tactics and the human factors that make organizations vulnerable, and frames this knowledge defensively to help security professionals recognize and resist such attacks.

SIST Guide Reference 100. A survey on large language model-based agents in autonomous, 2026. URL https://arxiv.org/html/2505.12786v2. This survey examines how large language model-based agents can be weaponized as autonomous cyberattack tools, analyzing their architecture across five core components: models, perception, memory, reasoning and planning, and tools. The authors document eight attack categories and map them across static infrastructure, mobile networks, and infrastructure-free systems such as blockchain and the metaverse.

SIST Guide Reference 101. Information warfare: An air force policy for the role of public affairs, 2026. URL https://media.defense.gov/2017/Dec/28/2001861671/-1/-1/0/T_0037_CRUMM_INFORMATION_WARFARE.PDF. The military's use or misuse of information in psychological or deception operations, under.

SIST Guide Reference 102. Information warfare and deception, 2026. URL https://www.inform.nu/Articles/Vol9/v9p213-223Hutchinson64.pdf. A 2006 paper by William Hutchinson published in the journal Informing Science. It examines the history of information warfare and the increasingly central role of deception within it, tracing the concept from its late-1980s origins as a technology-oriented military tactic for command-and-control dominance to a broader recognition of information itself as both weapon and target.

SIST Guide Reference 103. Military deception, 2026. URL https://www.jinfowar.com/tags/military-deception. A topic page from the Journal of Information Warfare collecting scholarly articles on military deception. Featured pieces argue that information operations officers should be conceptualized primarily as deception officers, and one quantitative reassessment reports that deception is employed in roughly 30 to 53 percent of military operations.

SIST Guide Reference 104. The utility of military deception and information operations, 2026. URL https://smallwarsjournal.com/2025/06/26/the-utility-of-military-deception/. An essay published in Small Wars Journal (June 2025) by a U.S. Army Civil Affairs officer arguing that military deception and information operations have become central to modern conflict.

SIST Guide Reference 105. Automated influence and the challenge of cognitive security, 2026. URL https://dl.acm.org/doi/10.1145/3384217.3385615. Sarah Rajtmajer and Daniel Susser, 'Automated Influence and the Challenge of Cognitive Security,' in Hot Topics in the Science of Security (HotSoS '20), April 2020, ACM. The paper argues that AI-powered computational propaganda poses national security threats that existing ethical frameworks do not address, and proposes 'cognitive security' as a productive conceptual lens for evaluating the ethics of automated influence operations and potential defensive responses.

SIST Guide Reference 106. Applications of the active inference and the free-energy principle, 2026. URL https://repository.tudelft.nl/file/File_e789366f-e00d-49c3-b0ef-333dd27356f3?preview=1. A 2024 bachelor's thesis by Lara Sakarya at Delft University of Technology presenting a systematic literature review of the active inference framework and the free-energy principle as applied to mimicking social human behavior in intelligent agents. It explains active inference as a theory describing behavior that minimizes surprise, and surveys model variants such as deep active inference, multimodal deep belief networks, predictive coding, and probabilistic programming.

SIST Guide Reference 107. Behavioral outcomes of human cognitive security, 2026. URL https://arxiv.org/html/2603.01355v1. An arXiv research paper (March 2026) proposing an integrative modeling framework for human cognitive security, defined as the degree to which people rely on truthful information to make truth-aligned judgments. It synthesizes Bayesian belief-updating with Prospect Theory to model how cognitive resources and emotional valuation shape behavior, and identifies three observable outcomes: veracity discernment, task-oriented actions, and information sharing.

SIST Guide Reference 108. Critical thinking techniques, 2026. URL https://www.cdse.edu/Portals/124/Documents/jobaids/insider/INT250-critical-thinking-techniques.pdf. A Tradecraft Primer: Structured Analytic Techniques for Improving. Intelligence Analysis.

SIST Guide Reference 109. The 'grey zone' and hybrid activities, 2026. URL http://connections-qj.org/article/grey-zone-and-hybrid-activities. This is a peer-reviewed article in Connections: The Quarterly Journal (Vol. 21, No. 2, Spring 2022) by Peter Dobias and Kyle Christensen examining military competition below the threshold of armed conflict. It analyzes how Russia, China, and Iran operate in the space between peace and war, describing Russia's emphasis on information measures, China's maritime and force approaches, and Iran's anti-access and proxy strategies.

SIST Guide Reference 110. A full spectrum of conflict design: How doctrine should embrace, 2026. URL https://irregularwarfare.org/articles/a-full-spectrum-of-conflict-design-how-doctrine-should-embrace-irregular-warfare/. An article by Dr. Robert S. Burrell on the Irregular Warfare Initiative arguing that U.S. military doctrine inadequately addresses gray zone and hybrid warfare. It proposes a two-dimensional framework spanning peace-to-war and direct-to-indirect means, yielding four approaches: traditional warfare, deterrence, irregular warfare, and competition.

SIST Guide Reference 111. Anonymous no more: Countering the gray zone threat - from mipb, 2026. URL https://mipb.ikn.army.mil/issues/continuous-transformation-2025/anonymous-no-more/. An article in the U.S. Army's Military Intelligence Professional Bulletin on countering gray zone threats. It discusses how adversaries operate below the threshold of open conflict using hybrid activities across tactical, operational, and strategic levels, and considers how military intelligence can identify and attribute actors who attempt to remain anonymous. The piece is framed around adapting intelligence practice to contemporary competition short of war.

SIST Guide Reference 112. Full text of "special forces unconventional warfare", 2026. URL https://archive.org/stream/SpecialForcesUnconventionalWarfare/Special%20Forces%20Unconventional%20Warfare_djvu.txt. This U.S. Army Training Circular (TC 18-01) defines the Special Forces concept for planning and conducting unconventional warfare operations, covering how units enable and support resistance movements in denied or hostile territory. It presents a seven-phase operational framework encompassing psychological preparation, infiltration, organization of underground and guerrilla forces, employment, and transition.

SIST Guide Reference 113. Fm 3-05.130 army special operations forces unconventional, 2026. URL https://www.bits.de/NRANEU/others/amd-us-archive/fm3-05.130(08).pdf. U.S. Army Field Manual FM 3-05.130, "Army Special Operations Forces Unconventional Warfare," published by Headquarters, Department of the Army in September 2008. The manual is organized into chapters covering an introduction to warfare types, the instruments of United States national power, national policy and doctrine, and planning considerations including the seven phases of unconventional warfare and the role of Army Special Operations Forces.

SIST Guide Reference 114. Army special operations forces unconventional warfare, 2026. URL https://irp.fas.org/doddir/army/fm3-05-130.pdf. FM 3-05.130, Army Special Operations Forces Unconventional Warfare (Headquarters, Department of the Army, 30 September 2008). The manual defines unconventional warfare and situates it within U.S. national power, covering the seven phases of UW operations, Special Forces missions, psychological operations, civil affairs operations in the UW context, and the roles of supporting elements including interagency partners. Distribution was restricted to U.S.

SIST Guide Reference 115. Army special operations forces intelligence, 2026. URL https://irp.fas.org/doddir/army/fm3-05-102.pdf. FM 3-05.102, Army Special Operations Forces Intelligence (Headquarters, Department of the Army). The manual addresses intelligence and electronic warfare (IEW) support across Army Special Operations Force components, covering Special Forces, Rangers, ARSOA, PSYOP, and Civil Affairs operations.

SIST Guide Reference 116. Army special operations forces intelligence, 2026. URL https://www.bits.de/NRANEU/others/amd-us-archive/fm3-05.102(01).pdf. A U.S. Army field manual, FM 3-05.102 (Army Special Operations Forces Intelligence), dated 2001 and superseding FM 34-36, distributed with restrictions to U.S. government agencies. The manual gives special operations forces commanders and staff a doctrinal overview of intelligence support to their missions, covering force structure, training, and operational requirements consistent with joint doctrine.

SIST Guide Reference 117. Office of strategic services (oss) manuals, 2026. URL https://smallwarsjournal.com/2025/11/09/office-of-strategic-services-oss-manuals-the-resistance-hub/. An article from Small Wars Journal (affiliated with Arizona State University) announcing that The Resistance Hub has compiled declassified Office of Strategic Services (OSS) manuals for public access. The OSS was the WWII predecessor to the CIA, and the documents illustrate how the United States organized clandestine activities in occupied Europe and Asia.

SIST Guide Reference 118. Special operations field manual, strategic services (provisional, 2026. URL https://archive.org/details/SpecialOperationsFieldManualStrategicServicesprovisional. A digitized World War II field manual from the Internet Archive, the Special Operations Field Manual, Strategic Services (provisional), issued July 18, 1944 by the U.S. Office of Strategic Services (OSS). The 32-page manual sets out the authorized functions, operational plans, methods, and organization of OSS Maritime Units and the broader Special Operations Branch.

SIST Guide Reference 119. office of strategic services - arsof history, 2026. URL https://arsof-history.org/pdf/book_office_of_strategic_services_primer_and_manuals.pdf. SIST guide bibliography entry.

SIST Guide Reference 120. Principles tradecraft, 2026. URL https://ia803205.us.archive.org/23/items/PrinciplesOfTradecraft/Principles%20of%20Tradecraft.pdf. Principles of Tradecraft, a 1995 publication by Militia Free Press (a subsidiary of The Resister). The document presents an overview of intelligence and espionage concepts, with chapters covering an introduction to espionage, agents (typology, identification, recruitment, and handling), and agent organization and management including personnel and structures. It is framed as an introductory treatment rather than a comprehensive reference on intelligence requirements.

SIST Guide Reference 121. How the kgb handled information - blockint, 2026. URL https://www.blockint.nl/methods/how-the-kgb-handled-information/. This is a Blockint blog post by Ludo Block, published in October 2022, analyzing a KGB training manual on information handling released by the Free Russia Foundation. The manual, written for foreign intelligence officers, sets out six requirements for valuable intelligence and a framework for evaluating sources based on past performance and competence.

SIST Guide Reference 122. The lubyanka files - free russia foundation think tank, 2026. URL https://thinktank.4freerussia.org/the-lubyanka-files/. SIST guide bibliography entry.

SIST Guide Reference 123. Full text of "kgb alpha team training manual" - internet archive, 2026. URL https://archive.org/stream/KGBAlphaTeamTrainingManual/KGB%20Alpha%20Team%20Training%20Manual_djvu.txt. A 1993 Paladin Press publication presenting a translated Soviet special-operations training text attributed to A. I. Dolmatov, accompanied by an extensive preface by Western trainer Jim Shortt. The preface traces the evolution of Soviet special forces from the 1917 revolution through the Cold War and describes organizations such as the KGB, MVD, and GRU and units including Alpha, Spetsnaz, and OMON.

SIST Guide Reference 124. The logician (the zinoviev's case). folder 46. the chekist, 2026. URL http://zinoviev.info/wps/archives/459. This article draws on the Mitrokhin Archive, compiled by defected KGB archivist Vasili Mitrokhin, to document Soviet state surveillance of dissident philosopher Alexander Zinoviev, who was assigned the codename Logician by the KGB's Fifth Chief Directorate. Zinoviev faced professional retaliation including revocation of his doctorate and expulsion from the Communist Party following the publication of satirical anti-Soviet works such as Yawning Heights.

SIST Guide Reference 125. Mitrokhin archive, 2026. URL https://wilson-center-digital-archive.dvincitest.com/topics/mitrokhin-archive. The Wilson Center Digital Archive link for the Mitrokhin Archive is a dead staging domain. The Mitrokhin Archive documents Soviet KGB history; use the published Cambridge University Press edition or Wilson Center production archive instead.

SIST Guide Reference 126. Mitrokhin archive, 2026. URL https://en.wikipedia.org/wiki/Mitrokhin_Archive. A Wikipedia article on the Mitrokhin Archive, a collection of handwritten notes made by KGB archivist Vasili Mitrokhin documenting Soviet intelligence operations from the 1930s through the 1980s. Mitrokhin secretly copied files between 1972 and 1984 while overseeing the relocation of KGB foreign intelligence archives, and after the Soviet collapse defected to the UK in 1992 with the material.

SIST Guide Reference 127. The mitrokhin archive : the kgb and the world, 2026. URL https://archive.org/details/mitrokhinarchive0000andr_c0s1. An Internet Archive record for The Mitrokhin Archive: The KGB and the World, a two-volume work by Christopher Andrew published in 1999 by Allen Lane, running to roughly 1,050 pages. The volumes draw on materials compiled by former KGB officer Vasili Mitrokhin to document Soviet intelligence operations, with the first volume covering the KGB in Europe and the West and the second addressing the KGB and the wider world.

SIST Guide Reference 128. Full text of "the secret war the office of strategic services in world, 2026. URL https://archive.org/stream/bub_gb_P3OIFS_yzyUC/bub_gb_P3OIFS_yzyUC_djvu.txt. An Internet Archive full-text scan of the proceedings of a 1991 National Archives conference on the Office of Strategic Services (OSS), the U.S.

SIST Guide Reference 129. Oss resources - office of strategic services society, 2026. URL https://www.osssociety.org/links.html. A resource directory page from the Office of Strategic Services Society, a historical organization dedicated to preserving the record of the WWII-era OSS. The page

functions as a curated library of links to external sites covering OSS history, including operations, related organizations, notable figures such as William Donovan and Allen Dulles, educational materials, and geographic theaters.

SIST Guide Reference 130. The official cia manual of trickery and deception, 2026. URL https://ia801604.us.archive.org/31/items/cia-manual-trickery-deception-2009/cia-manual-trickery-deception-2009.pdf. A reproduction of a Cold War-era manual written by magician John Mulholland for the CIA, presented with commentary by H. Keith Melton and Robert Wallace as "The Official CIA Manual of Trickery and Deception." The book situates the manual within the history of the MKULTRA program and the long-missing magic manuals, and reproduces Mulholland's guidance on applying sleight-of-hand and misdirection techniques to covert operational tasks.

SIST Guide Reference 131. Center for the study of intelligence - csi, 2026. URL https://www.cia.gov/resources/csi/. The Center for the Study of Intelligence (CSI) serves as a producer and repository of unclassified.

SIST Guide Reference 132. Studies in intelligence, 2026. URL https://www.cia.gov/resources/csi/studies-in-intelligence/. Studies in Intelligence is the CIA's professional journal, published by the Center for the Study of Intelligence (CSI). It covers historical, analytical, and methodological topics across the intelligence profession, and is issued quarterly in partially declassified extract form. As of 2026 the archive holds 110 issues, with the most recent being Volume 70, No. 1 (March 2026); articles are written by intelligence community professionals under their own names or pen names.

SIST Guide Reference 133. Studies in intelligence: New articles from the cia's in-house journal, 2026. URL https://nsarchive2.gwu.edu/NSAEBB/NSAEBB493/. This is a National Security Archive briefing book presenting declassified articles from the CIA's internal journal Studies in Intelligence, first published in 1955. The collection gathers articles obtained through Freedom of Information Act requests and litigation, spanning CIA history from the Kennedy era through the post-9/11 period.

SIST Guide Reference 134. What is your reading list for (counter)intelligence/tradecraft?, 2026. URL https://www.reddit.com/r/Intelligence/comments/cw1rav/what_is_your_reading_list_for/. How To Be A Spy: The WW2 SOE Training Manual - Denis Rigden The CIA Guide to Clandestine.

SIST Guide Reference 135. The origins of the ukusa agreement, 2026. URL https://unredacted.uk/briefings/ukusa-origins/. A briefing from Unredacted, a UK investigative outlet, covering the early development of the UKUSA Agreement, the postwar US-UK signals-intelligence framework that became the basis for the Five Eyes alliance. It traces the 1946 BRUSA agreement on intelligence exchange, Canada's negotiation toward equal partnership in 1949, and the gradual integration of Australia and New Zealand through the 1950s.

SIST Guide Reference 136. Mossad's secretive operations and reputation - facebook, 2026. URL https://www.facebook.com/groups/kakampinoy/posts/798254539769053/. The Mossad is concerned with foreign intelligence gathering, intelligence analysis.

SIST Guide Reference 137. [2601.12560] agentic artificial intelligence (ai), 2026. URL https://arxiv.org/abs/2601.12560. An arXiv paper surveying the shift from passive language models to Agentic AI, where large language models act as cognitive controllers that combine memory, tool use, and environmental feedback to pursue extended goals. It proposes a unified taxonomy organizing agent systems into six components: perception, brain, planning, action, tool use, and collaboration.

SIST Guide Reference 138. Agentic artificial intelligence (ai): Architectures, taxonomies, 2026. URL https://arxiv.org/html/2601.12560v1. An arXiv survey paper on agentic AI examining the shift from generative systems to autonomous agents that perceive, reason, plan, and act. It proposes a unified taxonomy decomposing LLM-based agents into six dimensions: core components, cognitive architecture, learning paradigms, multi-agent systems, environments and domains, and evaluation and safety.

SIST Guide Reference 139. Agentic ai design patterns by andrew ng, 2026. URL https://www.linkedin.com/posts/aishwarya-srinivasan_agentic-ai-design-patterns-are-emerging-as-activity-7336419057639772165-Uuni. A LinkedIn post by Aishwarya Srinivasan discussing agentic AI design patterns for building production-grade AI agents.

SIST Guide Reference 140. The agentic ai landscape and its conceptual foundations, 2026. URL https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/02/the-agentic-ai-landscape-and-its-conceptual-foundations_a9d4b451/396cf758-en.pdf. An OECD Artificial Intelligence Paper (No. 56, February 2026) titled "The Agentic AI Landscape and Its Conceptual Foundations," prepared by OECD staff with an expert group.

SIST Guide Reference 141. Agentic ai, explained, 2026. URL https://mitsloan.mit.edu/ideas-made-to-matter/agentic-ai-explained. An MIT Sloan explainer article on agentic AI, defining autonomous software systems that perceive, reason, and act to complete multi-step tasks with minimal human intervention. It distinguishes such agents from chatbots, cites a 2025 MIT Sloan/BCG survey finding 35% of companies had deployed agents with 44% planning to, and reviews business applications such as fraud detection and customer service.

SIST Guide Reference 142. Agentic ai: A comprehensive survey of architectures, applications, 2026. URL https://arxiv.org/abs/2510.25445. The arXiv abstract page for "Agentic AI: A Comprehensive Survey of Architectures, Applications," a 2025 paper by Mohamad Abou Ali and Fadi Dornaika. Based on a PRISMA systematic review of roughly 90 studies from 2018 to 2025, it proposes a dual-paradigm framework distinguishing symbolic/classical systems based on algorithmic planning and persistent state from neural/generative systems driven by stochastic generation and prompt orchestration.

SIST Guide Reference 143. Agentic ai architectures and design patterns | by anil jain, 2026. URL https://medium.com/@anil.jain.baba/agentic-ai-architectures-and-design-patterns-288ac589179a. A Medium article by Anil Jain (2025) surveying agentic AI system architectures and design patterns. It defines agentic AI as systems capable of independent decision-making, reviews frameworks such as LangChain, LlamaIndex, and AutoGen, and describes five system components: perception, decision-making, action, memory, and communication.

SIST Guide Reference 144. Agentic ai patterns and workflows on aws, 2026. URL https://docs.aws.amazon.com/prescriptive-guidance/latest/agentic-ai-patterns/introduction.html. An AWS Prescriptive Guidance document (July 2025) introducing agentic AI patterns and workflows. It presents reusable design templates for building AI agent systems that operate with autonomy while remaining controllable and aligned with goals, aimed at architects, developers, and product leaders.

SIST Guide Reference 145. A scalable design pattern for agentic ai systems, 2026. URL https://arxiv.org/html/2505.06817v1. This is an arXiv research paper by Sivasathivel Kandasamy titled "Control Plane as a Tool: A Scalable Design Pattern for Agentic AI Systems." It proposes an architectural pattern in which AI agents interact with a single control-plane interface that handles tool routing and selection, rather than exposing many tools directly.

SIST Guide Reference 146. Agentic ai frameworks: Key components & top 8 options in 2026, 2026. URL https://www.exabeam.com/explainers/agentic-ai/agentic-ai-frameworks-key-components-top-8-options/. An Exabeam explainer describing agentic AI frameworks as software toolkits that provide pre-built components and architectures for building autonomous AI agents. It outlines core elements such as agent coordination, tool integration, memory management, workflow definition, and deployment monitoring, and reviews eight frameworks including LangGraph, AutoGen, CrewAI, LlamaIndex, Haystack, DSPy, and Semantic Kernel.

SIST Guide Reference 147. Agent framework security, 2026. URL https://redteams.ai/topics/agentic-exploitation/agent-frameworks. Security analysis of major AI agent frameworks including LangChain, CrewAI, AutoGen, Semantic.

SIST Guide Reference 148. How riverside research advances agentic ai for national security, 2026. URL https://www.riversideresearch.org/insights/leaning-forward-how-riverside-research-advances-agentic-ai-for-national-security. This article by Riverside Research traces AI's evolution from large language models through retrieval-augmented systems, single-task agents, collaborative agentic systems, and toward emergent multi-agent autonomy capable of managing surveillance and decision support at operational speed.

SIST Guide Reference 149. What is agentic ai in security operations? autonomous soc agents, 2026. URL https://simbian.ai/blog/agentic-ai-security-operations-autonomous-soc-agents-explained. A 2025 blog article from Simbian AI explaining the application of agentic AI to security operations centers. It describes an architecture organized into perception, cognitive, and action modules, and a coordinated framework of specialized agents for tasks such as alert triage, threat investigation, and vulnerability management.

SIST Guide Reference 150. The right role for agentic ai in security operations, 2026. URL https://www.cybersecuritytribe.com/articles/the-right-role-for-agentic-ai-in-security-operations. An article from Cybersecurity Tribe examining where autonomous AI should and should not operate within security operations, drawing on survey data and commentary from numerous security experts. It identifies high-volume, repetitive tasks such as alert triage and policy validation as well suited to automation, while warning against autonomous handling of irreversible or high-impact decisions affecting infrastructure and access.

SIST Guide Reference 151. A practical guide to prebunking misinformation - inoculation science, 2026. URL https://inoculation.science/a-practical-guide-to-prebunking-misinformation/. A practitioner guide from Inoculation Science explaining prebunking as a proactive strategy to build preemptive resilience to misinformation. Grounded in inoculation theory, it describes how exposing people to weakened forms of manipulative content can help them develop resistance before they encounter it in the wild.

SIST Guide Reference 152. Social media experiment reveals potential to 'inoculate' millions, 2026. URL https://www.cam.ac.uk/stories/inoculateexperiment. A University of Cambridge news article describing a large study, conducted with Bristol University and Google's Jigsaw, testing whether short animated videos can help people resist online manipulation. The 90-second clips expose common manipulation techniques such as scapegoating, false dichotomies, and emotionally manipulative language, an approach the researchers call prebunking.

SIST Guide Reference 153. Agentic ai is exploding, but which framework should you bet on?, 2026. URL https://www.linkedin.com/posts/eordax_ai-genai-agents-activity-7357708242187149312-fBCO. The second half of the framework highlights common agentic frameworks.

SIST Guide Reference 154. Crewai, 2026. URL https://crewai.com. The homepage of CrewAI, a commercial platform for building, deploying, and managing AI agents at scale for enterprises. It presents the product as covering the full lifecycle from identifying automation opportunities to launching and optimizing multi-agent workflows while maintaining enterprise-level control.

SIST Guide Reference 155. Model context protocol (mcp): Security design considerations, 2026. URL https://www.nsa.gov/Portals/75/documents/Cybersecurity/CSI_MCP_SECURITY.pdf?ver=bmgiSbNQLP6Z_GiWtRt6bg%3D%3D. Radosevich and Halloran (2025) audit security vulnerabilities in Anthropic's Model Context Protocol (MCP), which allows LLMs to integrate with external tools and data sources. The authors demonstrate that language models using MCP can be manipulated through prompt injection to execute malicious code, enable remote access, and steal credentials.

SIST Guide Reference 156. Mcp security 101: A new protocol for agentic ai - protect ai, 2026. URL https://protectai.com/blog/mcp-security-101. A Protect AI blog post (April 2025) introducing the Model Context Protocol (MCP), the open-source layer Anthropic introduced in November 2024 to standardize how large language model applications connect to data sources and tools. The article explains how MCP acts as middleware between models and downstream services and surveys associated security risks, including overly broad permissions, unvetted servers, exposed endpoints, and limited monitoring.

SIST Guide Reference 157. Building agentic ai with mcp - bandwidth, 2026. URL https://www.bandwidth.com/blog/agentic-ai-mcp/. This is a Bandwidth blog post explaining how the Model Context Protocol (MCP) supports agentic AI systems that can assess context and take actions rather than only respond to prompts. Using a contact-center voice agent example, it describes MCP as a standard for letting AI models interact securely with external tools, APIs, and data sources, and covers instructions versus multi-step workflows.

SIST Guide Reference 158. Ai spotlight: Mcp (model context protocol) and agentic ai systems, 2026. URL https://www.gravitee.io/blog/mcp-model-context-protocol-agentic-ai. A Gravitee blog post explaining the Model Context Protocol (MCP), an open standard developed by Anthropic for how applications provide context and tools to large language models. It compares MCP to a universal connector that replaces custom per-tool integrations, describing an architecture of hosts, clients, and servers and benefits such as reusability, provider flexibility, and improved access controls. The post situates MCP within the broader growth of agentic AI systems.

SIST Guide Reference 159. Security risks of agentic ai: A model context protocol (mcp, 2026. URL https://businessinsights.bitdefender.com/security-risks-agentic-ai-model-context-protocol-mcp-introduction. A September 2025 Bitdefender Business Insights article by Martin Zugec examining security risks in the Model Context Protocol, the standard introduced by Anthropic for connecting AI agents to external tools and data. It identifies concerns including weak default authentication, supply-chain exposure from compromised tools, over-permissioned access tokens, injection and context-poisoning attacks, and gaps in audit logging for agentic workflows.

SIST Guide Reference 160. Breaking down the top 12 papers on agentic ai governance, 2026. URL https://www.linkedin.com/posts/oliver-patel_breaking-down-the-top-12-papers-on-agentic-activity-7355531066830376960-ynF3. Oliver Patel compiled a three-part series summarizing twelve influential research papers on governing autonomous AI systems, organized around themes of security and safety, infrastructure and principal-agent theory, and regulatory and capability assessment. The papers collectively argue that governance cannot be applied reactively after agents act but must instead be embedded at the architectural level, preventing unauthorized autonomous behavior before it occurs.

SIST Guide Reference 161. New governance frameworks offer a roadmap for managing risks, 2026. URL https://www.dwt.com/blogs/artificial-intelligence-law-advisor/2026/01/roadmap-for-managing-risks-unique-to-agentic-ai. A January 2026 article from the law firm Davis Wright Tremaine on governance frameworks for agentic AI. It argues that autonomous, adaptive AI systems pose distinct risks, such as unauthorized or erroneous actions, biased decisions, data breaches, and opaque audit trails, that require governance beyond existing AI frameworks.

SIST Guide Reference 162. Agentic ai report reveals need for reliable autonomous operations, 2026. URL https://www.dynatrace.com/news/blog/agentic-ai-report-reliable-autonomous-operations/. A Dynatrace blog post summarizing its Pulse of Agentic AI 2026 report, based on a survey of over 900 organizational leaders on enterprise adoption of agentic AI. It finds high adoption in IT operations alongside planned budget increases, while identifying barriers to scaling including security and compliance concerns, difficulty monitoring agents, and unclear autonomy boundaries.

SIST Guide Reference 163. Karl friston's groundbreaking research lays the foundation, 2026. URL https://deniseholt.us/verses-ais-groundbreaking-research-lays-the-foundation-for-shared-natural-super-intelligence/. An article on deniseholt.us covering a 2024 paper by VERSES AI researchers, led by Mahault Albarracin and co-authored by Karl Friston, titled Shared Protentions in Multi-Agent Active Inference. It explains how intelligent agents can develop shared, mutually aligned expectations about future states that enable coordinated group behavior without explicit communication, drawing on Husserl's work on temporal consciousness.

SIST Guide Reference 164. Verses to present research at active inference workshop, 2026. URL https://www.verses.ai/news/verses-to-present-research-at-the-5th-international-workshop-on-active-inference-iwai-2024. A press release from VERSES AI (August 2024) announcing that the

company would act as lead sponsor of and present research at the 5th International Workshop on Active Inference (IWAI 2024) in Oxford. It states that VERSES researchers had 12 accepted papers spanning foundational capabilities, multi-agent systems, applications, and ethics, and that the company's chief scientist Karl Friston would speak.

SIST Guide Reference 165. Unveiling the multifaceted concept of cognitive security, 2026. URL https://www.sciencedirect.com/science/article/pii/S0160791X25001460. We provide a comprehensive review of the current state of cognitive security.

SIST Guide Reference 166. Defining comprehensive cognitive security in the digital era: Literature review and concept analysis, 2026. URL https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5030171. Cognitive security, as an emerging field.

SIST Guide Reference 167. Unveiling the multifaceted concept of cognitive security, 2026. URL https://www.linkedin.com/posts/fran-casino-212783133_unveiling-the-multifaceted-concept-of-cognitive-activity-7341025497276895233-cJpS. A LinkedIn post by Fran Casino announcing a research article titled 'Unveiling the multifaceted concept of cognitive security: Trends, perspectives, and future challenges,' published in the Elsevier journal Technology in Society. The post describes the work as a literature review that analyzes definitions, challenges, and future trends in cognitive security and proposes a redefinition based on the concept's core components.

SIST Guide Reference 168. Darpa seeks proposals for intrinsic cognitive security program, 2026. URL https://potomacofficersclub.com/news/darpa-seeks-proposals-for-intrinsic-cognitive-security-program/. A Potomac Officers Club news article reporting on a DARPA request for proposals under its Intrinsic Cognitive Security program. The program seeks to protect mixed reality devices from cognitive attacks using mathematical approaches called formal methods, addressing risks such as flooding a device with information to induce motion sickness, distraction, or false alarms.

SIST Guide Reference 169. Ics | darpa, 2026. URL https://www.darpa.mil/research/programs/intrinsic-cognitive-security. This is an official DARPA program page for the Intrinsic Cognitive Security (ICS) program, which addresses vulnerabilities in mixed reality systems that could be exploited through cognitive attacks. The program aims to develop formal mathematical methods that guarantee mixed reality designs can protect users against adversarial interference.

SIST Guide Reference 170. Intrinsic cognitive security (ics) - highergov, 2026. URL https://www.highergov.com/grant-opportunity/intrinsic-cognitive-security-ics-350593/. A HigherGov listing for the DARPA Intrinsic Cognitive Security (ICS) research solicitation, which seeks to develop tactical mixed-reality systems that protect users against cognitive attacks using formal methods with cognitive safeguards. The program is structured as a 36-month effort in two 18-month phases, with defined funding ranges for a mixed-reality cognition technical area and an evaluation technical area.

SIST Guide Reference 171. Darpa preps program to protect mixed reality users, 2026. URL https://www.reddit.com/r/Futurology/comments/176yx4u/darpa_preps_program_to_protect_mixed_reality/. DARPA is putting together the Intrinsic Cognitive Security (ICS) research program "to build.

SIST Guide Reference 172. The ethics of cognitive security - yorkspace, 2026. URL https://yorkspace.library.yorku.ca/server/api/core/bitstreams/f82a16e0-41eb-4387-9517-dcc5277027c1/content. This 2023 York University doctoral dissertation by Andrew Ward Buzzell provides an ethical and epistemic assessment of state power exercised to defend against information threats, a domain the author terms cognitive security.

SIST Guide Reference 173. Epistemic security - elizabeth seger, 2026. URL https://elizabethseger.com/epistemic-security/. A project page from AI governance and ethics researcher Elizabeth Seger introducing the concept of epistemic security: protecting the processes through which information is created, distributed, and consumed in society. It discusses information threats to democracies such as disinformation, eroding trust in institutions, polarization, and the misuse of generative AI, and how technologies shape knowledge production.

SIST Guide Reference 174. Epistemic security 2029: Fortifying the uk's information supply, 2026. URL http://demos.co.uk/wp-content/uploads/2025/02/Epistemic-Security-2029_accessible.pdf. A February 2025 Demos report by Elizabeth Seger, Hannah Perry, and Jamie Hancock on strengthening the UK's information supply chain. It frames epistemic security, securing healthy and robust flows of trustworthy information, as essential to countering what it calls a democratic emergency driven by institutional distrust, the decline of local news, and concentrated control of information by social media platforms.

SIST Guide Reference 175. Tackling threats to informed decision- making in democratic societies, 2026. URL https://www.turing.ac.uk/sites/default/files/2020-10/epistemic-security-report_final.pdf. A 2020 Alan Turing Institute report, authored by Elizabeth Seger, Shahar Avin, and colleagues from Cambridge and the UK Defence Science and Technology Laboratory, on promoting epistemic security in technologically advanced democracies. It examines threats to informed decision-making and collective action, analyzing vulnerabilities in social epistemic infrastructures such as adversaries and blunderers, attention scarcity, group polarization, and the erosion of trust.

SIST Guide Reference 176. Understanding the neurocognitive mechanisms of cognitive security, 2026. URL https://www.sciencedirect.com/science/article/abs/pii/S014976342500449X. Cognitive security is a relatively new field that aims to understand and defend against.

SIST Guide Reference 177. Understanding the neurocognitive mechanisms of cognitive security, 2026. URL https://pubmed.ncbi.nlm.nih.gov/41167441/. A peer-reviewed review article published in Neuroscience & Biobehavioral Reviews (December 2025) by Crum and colleagues examining the neurocognitive mechanisms of cognitive security. The authors synthesize research on why people fall victim to false or deceptive information, proposing that certain brain systems are more exploitable than others.

SIST Guide Reference 178. Neuro-cognitive approaches to cybersecurity: a systematic review, 2026. URL https://www.emerald.com/ics/article/doi/10.1108/ICS-03-2024-0076/1332910/Neuro-cognitive-approaches-to-cybersecurity-a. A January 2026 systematic review in Information and Computer Security by the researcher Kritika, titled "Neuro-cognitive approaches to cybersecurity." It integrates findings from neuroscience and cognitive psychology to analyze the human factor in security, examining how cognitive and neurological insights can improve security awareness education, behavioral policy development, insider threat detection, and user interface design.

SIST Guide Reference 179. Survey of metrics for cognitive load in intelligence community, 2026. URL https://ncsu-las.org/2024/11/survey-of-metrics-for-cognitive-load-in-intelligence-community-settings/. An NCSU Laboratory for Analytic Sciences article summarizing a systematic survey of metrics for measuring cognitive load in intelligence-analysis and similar settings. Reviewing 125 articles published between 1998 and 2024, it identifies 129 distinct metrics grouped into non-biometric methods (questionnaires such as NASA-TLX, task performance, interaction tracking) and biometric methods (eye tracking, heart rate).

SIST Guide Reference 180. Why psychology of intelligence analysis still matters?, 2026. URL https://www.specialeurasia.com/2024/08/19/psychology-intelligence-analysis/. A SpecialEurasia article (2024) reviewing Richards J. Heuer Jr.'s 1999 work Psychology of Intelligence Analysis and arguing for its continued relevance. It summarizes Heuer's account of how cognitive biases such as confirmation bias, anchoring, and availability heuristics distort analytic judgment, and how analysts' backgrounds shape interpretation.

SIST Guide Reference 181. Effectiveness of training actions aimed at improving critical thinking, 2026. URL https://www.nature.com/articles/s41599-025-06143-6. Particularly noteworthy in this field is the resurgence of the cognitive inoculation theory.

SIST Guide Reference 182. Psychological inoculation for credibility assessment, sharing, 2026. URL https://pmc.ncbi.nlm.nih.gov/articles/PMC10498317/. A 2023 meta-analysis in the Journal of Medical Internet Research evaluating psychological inoculation, or prebunking, as a strategy against misinformation, drawing on 42 studies with over 42,000 participants. It reports bounded improvements in people's ability to distinguish misinformation from real information, while finding limited effect on intentions to share misinformation and leaving context, durability, and transfer conditions for review.

SIST Guide Reference 183. Prebunking interventions based on "inoculation" theory can reduce, 2026. URL https://misinforeview.hks.harvard.edu/article/global-vaccination-badnews/. A 2020 peer-reviewed study in the Harvard Kennedy School Misinformation Review by Roozenbeek, van der Linden, and Nygren testing the Bad News game as a prebunking intervention grounded in inoculation theory. Players take the role of a misinformation creator to learn common manipulation techniques such as impersonation, emotional appeals, polarization, and conspiratorial framing, building resistance to deceptive content.

SIST Guide Reference 184. Psychological inoculation against misinformation, 2026. URL https://jnnp.bmj.com/content/94/12/e2.40. Sander van der Linden is Professor of Social Psychology in Society in the Department of Psychology.

SIST Guide Reference 185. "inoculation" to resist misinformation - pubmed, 2026. URL https://pubmed.ncbi.nlm.nih.gov/38753337/. A 2024 JAMA Insights article by Sander van der Linden and Jon Roozenbeek on "inoculation" or prebunking as a psychological technique for resisting misinformation. Part of the journal's Communicating Medicine series, it describes how preparing audiences in advance can build cognitive resistance to misleading narratives, drawing an analogy to how vaccines build immunity.

SIST Guide Reference 186. Psychological inoculation against misinformation: Current evidence and future directions - cecilie s. traberg, jon roozenbeek, sander van der linden, 2022, 2026. URL https://journals.sagepub.com/doi/10.1177/00027162221087936. Much like a viral contagion, misinformation can spread rapidly from one individual to another.

SIST Guide Reference 187. Inoculation theory and misinformation, 2026. URL https://stratcomcoe.org/publications/download/Inoculation-theory-and-Misinformation-FINAL-digital-ISBN-ebbe8.pdf. A 2021 report published by the NATO Strategic Communications Centre of Excellence, authored by Jon Roozenbeek and Sander van der Linden of the Cambridge Social Decision-Making Lab, on inoculation theory and misinformation. It explores how psychology and behavioural science can help mitigate the spread of false and misleading information, noting that no single intervention through algorithms, legislation, or content moderation is sufficient.

SIST Guide Reference 188. From spycraft to self-mastery: How structured analytic techniques, 2026. URL https://spotterup.com/from-spycraft-to-self-mastery-how-structured-analytic-techniques-can-transform-everyday-decisions/. An article on Spotter Up by Eugene Nielsen arguing that structured analytic techniques (SATs) developed for intelligence analysis can improve everyday decision-making. It describes cognitive biases such as confirmation bias and overconfidence, then outlines categories of SATs including diagnostic, contrarian, imaginative, structuring, and decision-support methods.

SIST Guide Reference 189. A tradecraft primer - csi, 2026. URL https://www.cia.gov/resources/csi/books-monographs/a-tradecraft-primer/. This primer will assist analysts in dealing with the perennial problems of intelligence.

SIST Guide Reference 190. Objectivity - intelligence.gov, 2026. URL https://www.intelligence.gov/mission/our-values/objectivity. A page on Intelligence.gov, the U.S. Intelligence Community's public site, presenting objectivity as a core IC value. It explains that intelligence analysis must be performed and conveyed without distortion from personal or political bias, and references the standards codified in Intelligence Community Directive (ICD) 203 on analytic standards.

SIST Guide Reference 191. Richards heuer, 2026. URL https://en.wikipedia.org/wiki/Richards_Heuer. A Wikipedia biography of Richards J. Heuer Jr. (1927-2018), a long-serving CIA intelligence analyst known for foundational contributions to analytic tradecraft. It describes his development of the Analysis of Competing Hypotheses method, his book 'Psychology of Intelligence Analysis' arguing that structured tools help analysts cope with cognitive bias and uncertainty, and his co-authored guide to Structured Analytic Techniques.

SIST Guide Reference 192. The psychology of intelligence analysis, 2026. URL https://www.ialeia.org/docs/Psychology_of_Intelligence_Analysis.pdf. Psychology of Intelligence Analysis by Richards J. Heuer Jr., published by the Center for the Study of Intelligence, Central Intelligence Agency (1999). This foundational text examines the cognitive processes and mental limitations that affect intelligence analysts, focusing on how perception, memory, and bias shape judgment. It presents structured analytic methods intended to help analysts recognize and counteract these limitations and improve the quality of their reasoning.

SIST Guide Reference 193. Structured analytical techniques - organization of american states, 2026. URL https://www.oas.org/cicaddocs/Document.aspx?Id=2575. Heuer provides a number of starter questions in his book.

SIST Guide Reference 194. Structured analytic techniques for intelligence analysis, 2026. URL https://www.scribd.com/document/554459164/Structured-Analytic-Techniques-for-Intelligence-Analysis-by-Richards-and-Randolph. A copy of "Structured Analytic Techniques for Intelligence Analysis" hosted on Scribd, a roughly 310-page professional reference on analytical methodologies for intelligence work. It presents systematic frameworks that analysts can use to process information, test hypotheses, identify patterns, and reach evidence-based conclusions while reducing bias. The document is oriented toward practitioners seeking to strengthen analytic rigor.

SIST Guide Reference 195. Full article: Analytic tradecraft and the intelligence community, 2026. URL https://www.tandfonline.com/doi/full/10.1080/02684527.2012.746415. The emphasis and visibility afforded analytic tradecraft in the Intelligence Community's analytic.

SIST Guide Reference 196. Analytic tradecraft standards - army university press, 2026. URL https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/March-April-2021/Kwoun-Tradecraft-Standards/. The nine analytic tradecraft standards in Intelligence Community Directive (ICD) 203, Analytic.

SIST Guide Reference 197. Getting things done: The science behind stress-free productivity, 2026. URL https://www.sciencedirect.com/science/article/abs/pii/S0024630108000848. In 2001 David Allen proposed 'Getting Things Done' (GTD) as a method for enhancing personal.

SIST Guide Reference 198. Metoda gtd = getting things done - lukas barda, 2026. URL https://lukasbarda.cz/english/metoda-gtd-getting-things-done/. A Czech-language explainer of the Getting Things Done (GTD) productivity method created by David Allen. It describes the system's core steps of capturing thoughts, clarifying them into actionable items, organizing and prioritizing, regularly reviewing, and executing, including the principle of doing any task that takes under two minutes immediately. The page also surveys software tools for implementing GTD, such as Todoist, OmniFocus, Trello, Evernote, and Notion.

SIST Guide Reference 199. David allen explains why gtd improves team performance, 2026. URL https://www.youtube.com/watch?v=UE93vcMFFpc. SIST guide bibliography entry.

SIST Guide Reference 200. The science behind flow state | achieving optimal performance, 2026. URL https://us.dingbats-notebooks.com/blogs/the-dingbats-blog/the-science-behind-flow-state-achieving-optimal-performance-with-dingbats. A marketing blog post on the Dingbats Notebooks e-commerce site about flow state and how writing tools can support it. It summarizes Mihaly Csikszentmihalyi's concept of flow as a state of

full absorption marked by intense focus, clear goals, and immediate feedback, and reviews associated benefits and neuroscience such as reduced prefrontal-cortex activity and increased dopamine.

SIST Guide Reference 201. Go with the flow: A neuroscientific view on being fully engaged, 2026. URL https://pmc.ncbi.nlm.nih.gov/articles/PMC7983950/. A 2020 theoretical review article in the European Journal of Neuroscience by van der Linden, Tops, and Bakker proposing a neuroscientific model of flow, the state of full task absorption with strong drive and low self-referential thinking. The authors argue that the dopamine and norepinephrine systems drive the motivational and mood components of flow, and that interaction among the default mode, central executive, and salience networks produces its characteristic features.

SIST Guide Reference 202. Flow (psychology), 2026. URL https://en.wikipedia.org/wiki/Flow_(psychology). A Wikipedia article on flow, the psychological state of complete immersion and focused engagement in an activity, also known as being in the zone. It traces the concept to psychologist Mihaly Csikszentmihalyi and describes flow as a balance between challenge and skill, characterized by intense concentration, merging of action and awareness, loss of self-consciousness, a sense of control, distorted time perception, and intrinsic reward.

SIST Guide Reference 203. How flow theory unleashes high performance in your career, 2026. URL https://spiky.ai/en/blog/how-flow-theory-unleashes-high-performance-in-your-career. A blog article applying Mihaly Csikszentmihalyi's Flow Theory to workplace and career performance. It describes flow as a state of full absorption in an activity, lists conditions associated with it such as clear goals, immediate feedback, and a balance between challenge and skill, and discusses how time can appear distorted during flow. The piece argues that achieving flow states enhances productivity and job satisfaction across roles and industries.

SIST Guide Reference 204. The neuroscience of flow state: How the brain reaches peak, 2026. URL https://www.linkedin.com/pulse/neuroscience-flow-state-how-brain-reaches-peak-performance-sana-noor-doa2f. A LinkedIn article (Sana Noor, 2024) on the neuroscience of flow, the state of complete immersion in a task. It describes brain mechanisms associated with flow, including reduced prefrontal activity (transient hypofrontality) that lowers self-consciousness, dopamine-driven motivation, and deactivation of the default mode network to enable deep focus.

SIST Guide Reference 205. Flow research collective: Neuroscience of human performance, 2026. URL https://www.flowresearchcollective.com. This is the website of the Flow Research Collective, a research and development organization founded in 2018 that studies the neuroscience of human performance and brain health. It investigates flow states of focused absorption and applies that research to peak performance training for organizations as well as to mental health conditions such as PTSD and depression.

SIST Guide Reference 206. Investigating the "flow" experience: Key conceptual, 2026. URL https://pmc.ncbi.nlm.nih.gov/articles/PMC7033418/. A 2020 conceptual analysis by Sami Abuhamdeh in Frontiers in Psychology arguing that flow research has stalled because the construct is operationalized inconsistently across studies. It identifies disagreements over whether flow is a discrete state or a continuum, whether enjoyment is essential to it, and whether scales conflate flow's conditions with the experience itself.

SIST Guide Reference 207. The cognitive load - productivity tradeoff in task switching, 2026. URL https://discovery.researcher.life/article/the-cognitive-load-productivity-tradeoff-in-task-switching/e9ab764eba953a3195c078b42fdb73c4. A 2023 research article in the Proceedings of the Human Factors and Ergonomics Society Annual Meeting by Maximillian Chis and colleagues examining task switching during team-based search-and-rescue scenarios in Minecraft. Using an ACT-R model of working memory, the study found that teams switching between task sets less frequently showed both higher cognitive load and higher performance scores.

SIST Guide Reference 208. Securing industrial control systems: Components, cyber threats, 2026. URL https://pmc.ncbi.nlm.nih.gov/articles/PMC10649322/. This article provides a comprehensive overview of cybersecurity for Industrial Control Systems, covering SCADA, distributed control systems, and programmable logic controllers as they have evolved from isolated architectures to networked, cloud-connected deployments.

SIST Guide Reference 209. What are industrial control systems (ics)? | bitsight, 2026. URL https://www.bitsight.com/glossary/industrial-control-systems-ics. A glossary entry from the cybersecurity company Bitsight explaining Industrial Control Systems (ICS), defined as integrated hardware and software used to control, monitor, and automate industrial processes across manufacturing, energy, and critical infrastructure.

SIST Guide Reference 210. What are the differences between ot, ics, & scada security?, 2026. URL https://www.paloaltonetworks.com/cyberpedia/ot-vs-ics-vs-scada-security. A Palo Alto Networks Cyberpedia article explaining the relationship among operational technology (OT), industrial control system (ICS), and SCADA security.

SIST Guide Reference 211. The 2026 cybersecurity guide to industrial control systems - claroty, 2026. URL https://claroty.com/blog/cybersecurity-dictionary-industrial-control-systems-ics-security. A Claroty guide to securing industrial control systems (ICS) amid IT and operational technology convergence. It identifies challenges including an expanded attack surface, legacy systems lacking modern protections, third-party access gaps, patching delays due to uptime requirements, and advanced adversaries targeting ICS.

SIST Guide Reference 212. Operational technology cybersecurity - idaho national laboratory, 2026. URL https://inl.gov/national-security/cybersecurity/. SIST guide bibliography entry.

SIST Guide Reference 213. Ics matrix - mitre att&ck(r), 2026. URL https://attack.mitre.org/matrices/ics/. The Industrial Control Systems (ICS) domain of the MITRE ATT&CK framework, a knowledge base documenting adversary behaviors based on real-world observations of attacks on critical infrastructure. The matrix organizes methods into twelve tactical categories spanning initial access through impact, including ICS-specific concerns such as firmware modification and disruption of operational technology.

SIST Guide Reference 214. Cybersecurity using ics att&ck strategies, 2026. URL https://www.isa.org/intech-home/2021/june-2021/departments/cybersecurity-using-ics-att-ck-strategies. A June 2021 InTech Magazine article by Jacob Chapman, published by the International Society of Automation, on using the ICS ATT&CK framework to strengthen cybersecurity for manufacturing and industrial IoT systems. It describes a three-phase risk-management approach: gathering information on assets and network architecture, mapping potential attack paths to identify vulnerabilities, and prioritizing mitigations by impact.

SIST Guide Reference 215. Mitre att&ck for ics framework - dragos, 2026. URL https://www.dragos.com/mitre-attack-for-ics. A Dragos solutions page describing the MITRE ATT&CK for ICS framework, a knowledge base of adversary behaviors observed in attacks against industrial control system networks. It explains how the Dragos Platform maps detections to ATT&CK tactics and techniques through regular knowledge updates, profiles named threat groups, and organizes behaviors across tactic areas spanning initial access through impact scenarios such as loss of control, safety, or availability.

SIST Guide Reference 216. How to use the mitre att&ck framework for ics - nozomi networks, 2026. URL https://www.nozominetworks.com/resources/how-security-teams-use-the-mitre-attack-framework-for-ics. A Nozomi Networks resource (a 2020 webinar) on how security teams apply the MITRE ATT&CK framework for Industrial Control Systems. It explains that the ICS version is a community-sourced knowledge base mapping adversary tactics and behaviors specific to industrial environments, distinct from the IT-focused framework.

SIST Guide Reference 217. An evaluation framework for industrial control system cyber incidents, 2026. URL https://www.sciencedirect.com/science/article/abs/pii/S1874548221000718. We analyze six significant ICS cyber incidents in the energy and power industries, namely Stuxnet.

SIST Guide Reference 218. The cyber-physical six | honeywell, 2026. URL https://www.honeywell.com/content/dam/honeywellbt/en/documents/downloads/hon-corp-the-cyber-physical-six.pdf. An executive research report from Honeywell's Global Analysis, Research, and Defense group titled "The Cyber-Physical Six," tracing how targeted industrial attacks have evolved and predicting future trends. It reviews six landmark cyber-physical attacks affecting industrial control and operational technology systems, then analyzes observed trends such as modularity, expanding capabilities, and the increasing frequency of new attack tools.

SIST Guide Reference 219. Stuxnet 15 years later and the evolution of cyber threats to critical, 2026. URL https://homeland.house.gov/wp-content/uploads/2025/07/2025-07-22-CIP-Testimony.pdf. I've been asked specifically to describe how.

SIST Guide Reference 220. Zetter details how stuxnet marked a turning point in cyberwarfare, 2026. URL https://industrialcyber.co/industrial-cyber-attacks/zetter-details-how-stuxnet-marked-a-turning-point-in-cyberwarfare-by-enabling-physical-sabotage-through-code/. Journalist Kim Zetter testified before Congress on how Stuxnet demonstrated that physical infrastructure could be destroyed through malicious code alone, targeting Siemens programmable logic controllers at Iran's Natanz uranium enrichment facility.

SIST Guide Reference 221. About, 2026. URL https://www.odni.gov/index.php/ic-legal-reference-book/presidential-policy-directive-28/123-about. Presidential Policy Directive 28 (PPD-28), Signals Intelligence Activities, in the ODNI IC Legal Reference Book, establishing principles and safeguards (data minimization and protections for personal information regardless of nationality) that govern U.S. signals intelligence collection and use.

SIST Guide Reference 222. Cia - national archives, 2026. URL https://www.archives.gov/files/isoo/fcgr/cia.pdf. The scope of the CIA mission is vast and the complexities of intelligence tradecraft.

SIST Guide Reference 223. Active-measures-and-information-wars - central intelligence agency, 2026. URL https://www.cia.gov/resources/csi/static/active-measures-and-information-wars.pdf. A book review article by J. E. Leonardson (a CIA Directorate of Analysis analyst writing under a pen name), published in Studies in Intelligence Vol. 64, No. 1 (March 2020).

SIST Guide Reference 224. Cyber kill chain(r) | lockheed martin, 2026. URL https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. A Lockheed Martin capabilities page describing the Cyber Kill Chain, a framework that is part of the company's Intelligence Driven Defense model for identifying and preventing cyber intrusions. It frames intrusions as a sequence of stages an adversary must complete to achieve an objective, with the aim of improving defenders' visibility into attacker behavior, and is oriented toward defending against advanced persistent threats.

SIST Guide Reference 225. Ai agents vs. agentic ai: A conceptual taxonomy, applications, 2026. URL https://www.sciencedirect.com/science/article/pii/S1566253525006712. Illustration of the three core characteristics defining AI Agents: autonomy, task-specificity.

SIST Guide Reference 226. Agentic ai: A comprehensive survey of technologies, applications, 2026. URL https://www.semanticscholar.org/paper/Agentic-AI:-A-Comprehensive-Survey-of-Technologies,-Pati/bb10ee1cf6d645ad74b9b35bb916086e6b3e340c. A robust multidimensional taxonomy is proposed that classifies agents based on their structural.

SIST Guide Reference 227. Ai agent frameworks: Choosing the right foundation for your ... - ibm, 2026. URL https://www.ibm.com/think/insights/top-ai-agent-frameworks. An IBM Think Insights article comparing leading AI agent frameworks to help teams choose a foundation for building agentic systems. It surveys open-source orchestration frameworks for single- and multi-agent solutions, including CrewAI and AutoGen, and discusses considerations such as workflow orchestration, collaboration among agents, and integration. The article is written as a practitioner-oriented overview of the framework landscape.

SIST Guide Reference 228. Agi-edgerunners/llm-agents-papers, 2026. URL https://github.com/AGI-Edgerunners/LLM-Agents-Papers. A curated GitHub repository (AGI-Edgerunners/LLM-Agents-Papers) collecting research papers on large language model based agents, last updated July 2025. It organizes work into categories including survey papers, enhancement techniques such as planning, memory, feedback, retrieval, and search, agent interactions like tool usage and conversation, domain applications, training methods, multi-agent systems, safety, and benchmarks.

SIST Guide Reference 229. How different types of ai agents work - [x]cube labs, 2026. URL https://www.xcubelabs.com/blog/how-different-types-of-ai-agents-work-a-comprehensive-taxonomy-and-guide/. It explores the taxonomy of agents, bridging the gap between classical artificial intelligence.

SIST Guide Reference 230. Karl friston explains active inference & ai breakthroughs - youtube, 2026. URL https://www.youtube.com/watch?v=Q2O1iNCQadI. A YouTube episode of "Karl's Corner" featuring Dr. Karl Friston, Chief Scientist at VERSES, explaining active inference and its implications for AI. He contrasts active inference, in which systems build internal models of the world to understand cause and effect, with prevailing AI approaches that mainly mimic patterns in data, and discusses claims of substantially improved performance and efficiency.

SIST Guide Reference 231. The secret history of disinformation and political warfare - csi, 2026. URL https://www.cia.gov/resources/csi/studies-in-intelligence/volume-64-no-1/active-measures-the-secret-history-of-disinformation-and-political-warfare/. The CIA Studies in Intelligence URL for 'The Secret History of Disinformation' returns 404. The article by Thomas Rid on political warfare history is accessible through the CIA CSI portal at an updated path; verify the URL before citation.

SIST Guide Reference 232. European ai office, 2026. URL https://digital-strategy.ec.europa.eu/en/policies/ai-office. The European AI Office is the European Commission's central hub for developing and implementing AI governance across the EU, established to support trustworthy AI adoption while protecting people from associated risks. Its responsibilities include enforcing regulations for general-purpose AI models, implementing the AI Act, developing evaluation tools and benchmarks for assessing AI capabilities, and investigating potential regulatory violations.

SIST Guide Reference 233. General-purpose ai code of practice, 2026. URL https://digital-strategy.ec.europa.eu/en/policies/ai-code-practice. An official European Commission Digital Strategy webpage documenting the General-Purpose AI Code of Practice, a voluntary guidance document helping general-purpose AI providers comply with the EU AI Act's rules on safety, transparency, and copyright. It describes an iterative drafting process involving nearly 1,000 stakeholders across four working groups, running from September 2024 through July 2025.

SIST Guide Reference 234. Ai act, 2026. URL https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai. The European Commission's official page on the AI Act, described as the first comprehensive legal framework on artificial intelligence worldwide. It explains the regulation's risk-based approach, classifying AI systems into unacceptable, high, transparency, and minimal risk tiers, with prohibited practices and strict requirements for high-risk uses.

SIST Guide Reference 235. Iso/iec 42005:2025 ai system impact assessment, 2026. URL https://www.iso.org/standard/44545.html. ISO standard page for AI system impact assessment.

SIST Guide Reference 236. Iso/iec tr 24028:2020 artificial intelligence trustworthiness overview, 2026. URL https://www.iso.org/standard/77608.html. The ISO catalog page for ISO/IEC TR 24028:2020, a technical report titled "Information technology - Artificial intelligence - Overview of trustworthiness in artificial intelligence." The document surveys topics related to AI trustworthiness, including approaches to establishing trust through transparency, explainability, and controllability, and approaches to assess and achieve availability, resilience, reliability, accuracy, safety, security, and privacy of AI systems.

SIST Guide Reference 237. Artificial intelligence: An accountability framework for federal agencies and other entities, 2026. URL https://www.gao.gov/products/gao-21-519sp. Official GAO AI accountability framework.

SIST Guide Reference 238. Recommendation on the ethics of artificial intelligence, 2026. URL https://www.unesco.org/en/artificial-intelligence/recommendation-ethics. The official UNESCO page for the Recommendation on the Ethics of Artificial Intelligence, the first global standard-setting instrument on AI ethics, adopted in 2021 and applicable to all 194 member states. It outlines four core values, including human rights protection and environmental flourishing, and ten guiding principles such as proportionality, privacy, transparency, and fairness.

SIST Guide Reference 239. Digital space and human rights, 2026. URL https://www.ohchr.org/en/digital-space-and-human-rights. Official OHCHR digital rights portal.

SIST Guide Reference 240. The right to privacy in the digital age, 2026. URL https://www.ohchr.org/en/privacy-in-the-digital-age. The Office of the High Commissioner for Human Rights (OHCHR) hub page on the right to privacy in the digital age. It addresses how data-intensive technologies, particularly artificial intelligence, create risks for privacy, autonomy, and human dignity, and curates international standards, reports, and expert consultations.

SIST Guide Reference 241. Modernised convention 108, 2026. URL https://www.coe.int/en/web/data-protection/convention108/modernised. Official Council of Europe Convention 108+ source.

SIST Guide Reference 242. Guidance for generative ai in education and research, 2026. URL https://unesdoc.unesco.org/ark:/48223/pf0000386693. Official UNESCO generative AI education guidance.

SIST Guide Reference 243. Ai competency frameworks for teachers and students, 2026. URL https://www.unesco.org/en/articles/unesco-launches-new-ai-competency-frameworks-students-and-teachers. A UNESCO announcement of two new AI competency frameworks, one for students and one for teachers, intended to guide safe and responsible engagement with artificial intelligence in education. The student framework emphasizes a human-centered perspective, ethical use, foundational AI knowledge, and design thinking, while the teacher framework covers ethics, technical understanding, and pedagogy.

SIST Guide Reference 244. Ai and education, 2026. URL https://www.unesco.org/gem-report/en/ai-and-education. Official UNESCO GEM AI and education source hub.

SIST Guide Reference 245. Artificial intelligence in education, 2026. URL https://www.oecd.org/en/topics/sub-issues/artificial-intelligence-in-education.html. Official OECD AI in education topic page.

SIST Guide Reference 246. Digital education action plan 2021-2027, 2026. URL https://education.ec.europa.eu/focus-topics/digital-education/action-plan. The European Commission's official page on the Digital Education Action Plan (2021-2027), a strategic framework for promoting high-quality, inclusive digital learning across EU education systems. It defines digital education as the use of digital tools, technologies, and content to support teaching, learning, and assessment, and cites pandemic-driven adoption alongside persistent gaps in teacher readiness, student digital skills, and household access.

SIST Guide Reference 247. Ai in the public sector, 2026. URL https://oecd.ai/en/themes/public-sector. Official OECD.AI public-sector AI theme page.

SIST Guide Reference 248. Artificial intelligence working group, 2026. URL https://www.worldbank.org/en/programs/govtech/artificial-intelligence. The World Bank GovTech program page for its Artificial Intelligence Working Group, a community of government technology experts focused on knowledge-sharing and policy tools for responsible public-sector AI adoption. It notes that many developing countries face barriers such as limited digital skills, infrastructure, and data, which risk widening global inequality.

SIST Guide Reference 249. Govtech: Putting people first, 2026. URL https://www.worldbank.org/en/programs/govtech. The official page for the World Bank's Global Program on GovTech and Public Sector Innovation, which helps governments use technology and data to improve public services and governance. It describes support for digital transformation in public administration across areas such as tax administration, public financial management, human resource systems, and citizen engagement, with cross-cutting themes including responsible AI and green digital transformation.

SIST Guide Reference 250. Ai guide for government, 2026. URL https://ai.gov/. The official U.S. government AI.gov website presenting the federal administration's artificial intelligence strategy. It is organized around an AI Action Plan built on three pillars: accelerating innovation, building infrastructure, and leading international AI diplomacy. The site compiles executive orders, policy documents and OMB memos on government AI adoption, education initiatives, and leadership remarks, framing AI development as central to U.S. global competitiveness.

SIST Guide Reference 251. European data governance act, 2026. URL https://digital-strategy.ec.europa.eu/en/policies/data-governance-act. The European Commission page explaining the Data Governance Act, an EU regulation that became applicable in September 2023 to build trust in data sharing and ease reuse of data. It outlines four mechanisms: facilitating reuse of protected public-sector data, establishing trusted data intermediaries, enabling voluntary data sharing by citizens and businesses, and removing barriers to cross-sector and cross-border data use.

SIST Guide Reference 252. Data act explained, 2026. URL https://digital-strategy.ec.europa.eu/en/policies/data-act-explained. An official European Commission explainer on the EU Data Act, which became applicable on 12 September 2025.

SIST Guide Reference 253. Common european data spaces, 2026. URL https://digital-strategy.ec.europa.eu/en/policies/data-spaces. This is an official European Commission webpage describing the Common European Data Spaces initiative, part of the EU strategy to create interconnected, trustworthy data-sharing environments across strategic sectors. It explains that data spaces let organizations and individuals share data while retaining control, guided by principles of open participation, privacy protection, and fair access rules.

SIST Guide Reference 254. A european strategy for data, 2026. URL https://digital-strategy.ec.europa.eu/en/policies/strategy-data. An official European Commission page outlining the European Strategy for Data, which aims to create a single market for data to support competitiveness and data sovereignty. It describes initiatives such as Common European Data Spaces, opening high-value public datasets, and investment in cloud and data-processing capacity, supported by the Data Governance Act and the Data Act. The page frames data sharing as a driver of innovation balanced with privacy and European values.

SIST Guide Reference 255. Web of things (wot) architecture 1.1, 2026. URL https://www.w3.org/TR/wot-architecture11/. The W3C Recommendation for Web of Things Architecture 1.1, published in December 2023, defining an abstract architecture for interoperability across diverse Internet of Things platforms. It introduces core concepts including Things described by machine-readable Thing Descriptions, reusable Thing Models, and Consumers that interpret descriptions to interact via Properties, Actions, and Events.

SIST Guide Reference 256. Web of things (wot) thing description 1.1, 2026. URL https://www.w3.org/TR/wot-thing-description11/. The W3C WoT Thing Description 1.1 is a formal information model and standardized representation format enabling IoT devices to describe their metadata and interaction capabilities in a machine-readable way, facilitating interoperability across diverse ecosystems.

SIST Guide Reference 257. Web of things (wot) discovery, 2026. URL https://www.w3.org/TR/wot-discovery/. A W3C Recommendation for Web of Things (WoT) Discovery, published December 5, 2023 by the W3C Web of Things Working Group. It specifies how IoT devices and services can be discovered and how their Thing Description metadata can be accessed securely, using a two-phase model of Introduction and Exploration.

SIST Guide Reference 258. Openapi specification, 2026. URL https://spec.openapis.org/oas/. The official OpenAPI Initiative publications page, serving as a central index for the OpenAPI Specification and related standards including the Arazzo and Overlay specifications. It provides access to multiple specification versions (2.0, 3.0, 3.1, and 3.2) and their corresponding downloadable schemas identified by release date, along with a registry of extensions, formats, media types, and other resources.

SIST Guide Reference 259. Verifiable credentials data model v2.0, 2026. URL https://www.w3.org/TR/vc-data-model-2.0/. The W3C Verifiable Credentials Data Model v2.0 Recommendation, which specifies how to express digital credentials on the web in a cryptographically secure, privacy-respecting way. It defines an extensible data model for tamper-evident assertions made by an issuer about a subject, within a three-party ecosystem of issuers, holders, and verifiers supported by verifiable data registries.

SIST Guide Reference 260. Decentralized identifiers (dids) v1.0, 2026. URL https://www.w3.org/TR/did-core/. The W3C Recommendation for Decentralized Identifiers (DIDs) v1.0, published July 2022, defining a type of identifier that enables verifiable digital identity without reliance on a centralized registration authority. It specifies DID syntax (a scheme, method name, and method-specific identifier) and the DID document data model, which expresses verification methods, services, controllers, and verification relationships for authentication and assertion.

SIST Guide Reference 261. Rfc 9110: Http semantics, 2026. URL https://www.rfc-editor.org/rfc/rfc9110.html. RFC 9110, the official IETF standards document defining the core semantics and architecture of HTTP, published in June 2022 and consolidating nine earlier RFCs. It establishes terminology and protocol aspects shared across HTTP versions, including methods, status codes, header fields, content negotiation, conditional and range requests, authentication, and the http and https URI schemes.

SIST Guide Reference 262. Artificial intelligence, 2026. URL https://www.ilo.org/topics-and-sectors/artificial-intelligence. The International Labour Organization's topic portal on artificial intelligence and the world of work. It examines AI's dual role in automating worker tasks and in automating managerial functions through algorithmic management, arguing that whether AI displaces or complements jobs depends on how technology is integrated into work processes.

SIST Guide Reference 263. Mind the ai divide: Shaping a global perspective on the future of work, 2026. URL https://www.ilo.org/publications/major-publications/mind-ai-divide-shaping-global-perspective-future-work. A joint UN and International Labour Organization report (July 2024) titled 'Mind the AI Divide,' examining how unequal AI adoption can deepen global inequality. It argues that disparities in digital infrastructure, technology, education, and training risk leaving less developed nations further behind as economies shift toward AI-driven production.

SIST Guide Reference 264. Global commission on the future of work, 2026. URL https://www.ilo.org/resource/news/global-commission-future-work. An International Labour Organization news article (January 2019) announcing the findings of the ILO Global Commission on the Future of Work, a 15-month study co-chaired by the leaders of South Africa and Sweden. The commission issued ten recommendations addressing workplace change driven by technological and demographic shifts, including universal labor protections, lifelong learning, and stronger social safety nets.

SIST Guide Reference 265. Ai and work, 2026. URL https://oecd.ai/en/work. Official OECD.AI work theme page.

SIST Guide Reference 266. Prov overview, 2026. URL https://www.w3.org/TR/prov-overview/. A W3C Working Group Note from 2013 that provides an overview and roadmap for the PROV family of specifications for representing and exchanging provenance information on the web. It defines provenance as information about the entities, activities, and people involved in producing data, used to assess quality, reliability, and trustworthiness.

SIST Guide Reference 267. Prov-o: The prov ontology, 2026. URL https://www.w3.org/TR/prov-o/. The W3C Recommendation for PROV-O, published in April 2013, which expresses the PROV data model as an OWL2 ontology for representing provenance information across systems. It defines three core classes, Entity, Activity, and Agent, and organizes terms into starting-point, expanded, and qualified categories.

SIST Guide Reference 268. Data catalog vocabulary (dcat) version 3, 2026. URL https://www.w3.org/TR/vocab-dcat-3/. DCAT Version 3 is a W3C RDF vocabulary designed to facilitate interoperability between data catalogs published on the web, enabling organizations to describe datasets and data services using standardized terminology for improved discoverability and federated search. The specification organizes catalog metadata around seven core classes including Catalog, Dataset, Distribution, Data Service, and Dataset Series, drawing on established vocabularies such as Dublin Core and FOAF.

SIST Guide Reference 269. Data on the web best practices, 2026. URL https://www.w3.org/TR/dwbp/. A W3C Recommendation, "Data on the Web Best Practices," published January 31, 2017 by the Data on the Web Best Practices Working Group. It offers 35 best practices for publishing and consuming data on the Web, covering metadata, licensing and provenance, data quality, dataset versioning, persistent URIs, machine-readable formats, vocabulary reuse, access methods, preservation, and feedback.

SIST Guide Reference 270. Nist big data interoperability framework, 2026. URL https://www.nist.gov/programs-projects/big-data-interoperability-framework. NIST Special Publication 1500-1 (revised edition by Chang and Grady) establishes foundational terminology and consensus definitions for Big Data through the NIST Big Data Public Working Group. The volume defines Big Data characteristics, taxonomy, and a reference architecture assigning roles to Application Providers, Data Consumers, Data Providers, and System Orchestrators.

SIST Guide Reference 271. Datacite metadata schema, 2026. URL https://schema.datacite.org/. The DataCite Metadata Schema page, introducing a standardized framework of core metadata properties chosen for accurate and consistent identification of research resources for citation and retrieval. It notes the latest version, 4.7 (March 2026), which adds resource types such as Poster and Presentation along with new identifier and relation-type options.

SIST Guide Reference 272. C2pa specifications, 2026. URL https://c2pa.org/specifications/specifications/. The specifications hub for the C2PA (Coalition for Content Provenance and Authenticity), a standards initiative that develops technical methods for certifying the source and history of media content to counter misleading information. It publishes the core Content Credentials specification along with related material such as attestations and a soft-binding API, plus implementation, security, and user-experience guidance including for AI-generated content.

SIST Guide Reference 273. Wcag 2 overview, 2026. URL https://www.w3.org/WAI/standards-guidelines/wcag/. The W3C Web Accessibility Initiative overview of the Web Content Accessibility Guidelines (WCAG), an international standard for making web content accessible to people with disabilities. It explains that WCAG is organized around four principles (perceivable, operable, understandable, robust) with testable success criteria at three conformance levels (A, AA, AAA), and covers versions 2.0, 2.1, and 2.2.

SIST Guide Reference 274. Cast universal design for learning guidelines version 3.0, 2026. URL https://udlguidelines.cast.org/. The official CAST website for the Universal Design for Learning (UDL) Guidelines version 3.0, released in 2024. The framework offers research-based guidance for designing inclusive learning environments and is organized around three principles: Engagement (motivation and emotional support), Representation (accessible presentation of information), and Action and Expression (diverse means of participation and communication).

SIST Guide Reference 275. Fact sheet: New rule on the accessibility of web content and mobile apps provided by state and local governments, 2026. URL https://www.ada.gov/resources/2024-03-08-web-rule/. A US Department of Justice fact sheet explaining the 2024 ADA Title II rule requiring state and local governments to make their web content and mobile apps accessible. It establishes WCAG 2.1 Level AA as the technical standard, applies to entities such as schools, courts, libraries, and transit agencies, and sets compliance deadlines of April 2027 for larger jurisdictions and April 2028 for smaller ones.

SIST Guide Reference 276. What is a data protection impact assessment and when is this mandatory?, 2026. URL https://www.edpb.europa.eu/sme-data-protection-guide/faq-frequently-asked-questions/answer/what-data-protection-impact_en. A European Data Protection Board FAQ page, part of its data protection guide for small businesses, explaining Data Protection Impact Assessments (DPIAs) and when they are mandatory. It describes a DPIA as a written assessment of the impact of a planned processing operation, required when processing poses high risks to individuals' rights.

SIST Guide Reference 277. Endorsed wp29 guidelines, 2026. URL https://www.edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines_en. This is a European Data Protection Board webpage listing guidelines and documents originating from the Article 29 Working Party that the EDPB endorsed at its first plenary meeting. The catalogued materials relate to the GDPR and cover topics such as consent and transparency, data breach notification, automated decision-making and profiling, data protection impact assessments, data protection officers, and binding corporate rules.

SIST Guide Reference 278. Recommendation of the council on public procurement, 2026. URL https://legalinstruments.oecd.org/api/print?ids=320&lang=en. The OECD Recommendation of the Council on Public Procurement (OECD/LEGAL/0411), a legal instrument adopted by the OECD Council in 2015 on the proposal of the Public Governance Committee. It frames public procurement as a pillar of strategic governance and service delivery and sets out principles for governments to follow.

SIST Guide Reference 279. Open contracting data standard, 2026. URL https://standard.open-contracting.org/latest/en/. The documentation homepage for the Open Contracting Data Standard, version 1.1.5, maintained by the Open Contracting Partnership to support disclosure of government contracting data across the procurement lifecycle. It provides a common data model spanning planning, tender, award, contract, and implementation stages, along with a primer, implementation guidance, technical schemas, and validation tooling.

SIST Guide Reference 280. Nist sp 800-61 rev. 3: Incident response recommendations and considerations for cybersecurity risk management, 2026. URL https://csrc.nist.gov/pubs/sp/800/61/r3/final. NIST SP 800-61 Rev. 3, published April 2025, integrates incident response guidance into broader cybersecurity risk management aligned with the NIST Cybersecurity Framework 2.0, superseding the 2012 Rev. 2. The publication addresses cyber threat information sharing, incident handling and management practices, and procedures for detecting, responding to, and recovering from security incidents.

SIST Guide Reference 281. Artificial intelligence cybersecurity challenges, 2026. URL https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges. An ENISA (European Union Agency for Cybersecurity) report published December 15, 2020 mapping the cybersecurity challenges of artificial intelligence. It defines AI scope through a lifecycle approach, identifies the assets requiring protection within AI ecosystems, and develops a threat taxonomy classified across lifecycle stages and asset categories.

SIST Guide Reference 282. Ai research: Security and resilience, 2026. URL https://www.nist.gov/artificial-intelligence/ai-research-security-and-resilience. A NIST page on AI research focused on security and resilience, framing these as core characteristics of trustworthy AI under the NIST AI Risk Management Framework.

SIST Guide Reference 283. Recommendation of the council on open government, 2026. URL https://legalinstruments.oecd.org/api/print?ids=359&lang=en. An OECD legal instrument document reproducing the Recommendation of the Council on Open Government (OECD/LEGAL/0438), adopted on 14 December 2017. It defines open government as a culture of governance promoting transparency, integrity, accountability, and stakeholder participation in support of democracy and inclusive growth.

SIST Guide Reference 284. Verifiable credential data integrity 1.0, 2026. URL https://www.w3.org/TR/vc-data-integrity/. The W3C Recommendation for Verifiable Credential Data Integrity 1.0, published May 2025, defining mechanisms for ensuring the authenticity and integrity of verifiable credentials using cryptographic proofs. It specifies a process of data transformation, hashing, and proof generation, and a corresponding verification procedure, along with a proof data model containing properties such as type, verification method, purpose, and proof value.

SIST Guide Reference 285. Nist ai resource center, 2026. URL https://airc.nist.gov/. The NIST AI Resource Center (AIRC), a government platform supporting implementation of the NIST AI Risk Management Framework, a voluntary framework for managing AI risk. It provides the core framework along with a playbook of practical actions, profiles tailored to specific sectors and technologies, use cases, and crosswalks linking the framework to other governance structures.

SIST Guide Reference 286. Model cards for model reporting, 2026. URL https://arxiv.org/abs/1810.03993. The arXiv abstract for "Model Cards for Model Reporting" (2018) by Mitchell, Wu, Zaldivar, and colleagues, which introduces a framework for transparent documentation of machine learning models. Model cards are short accompanying documents that report a model's benchmarked performance across varied conditions, including different cultural, demographic, and phenotypic groups, along with intended use, evaluation methodology, and deployment considerations.

SIST Guide Reference 287. Datasheets for datasets, 2026. URL https://arxiv.org/abs/1803.09010. A 2018 arXiv paper proposing 'datasheets for datasets,' a standardized documentation framework for machine learning datasets modeled on electronic component datasheets. The authors argue the field lacks consistent dataset documentation, which creates risk in high-stakes applications, and propose that datasets be accompanied by documentation covering motivation, composition, collection process, recommended uses, and test results.

SIST Guide Reference 288. Algorithmic transparency recording standard hub, 2026. URL https://www.gov.uk/government/collections/algorithmic-transparency-recording-standard-hub. A GOV.UK collection page serving as the hub for the UK Algorithmic Transparency Recording Standard (ATRS), maintained by the Government Digital Service. It provides a standardized template for documenting public-sector use of algorithmic tools, completion guidance, policy on scope and compliance, and a searchable repository of published transparency records.

SIST Guide Reference 289. Guidance for organisations using the algorithmic transparency recording standard, 2026. URL https://www.gov.uk/government/publications/guidance-for-organisations-using-the-algorithmic-transparency-recording-standard. This is a GOV.UK guidance page published by the Government Digital Service that instructs public sector organizations on completing the Algorithmic Transparency Recording Standard (ATRS) template and publishing their records to the GOV.UK repository. It applies both to central government bodies required to publish under mandatory policy and to other public sector bodies doing so voluntarily.

SIST Guide Reference 290. Nist sp 800-218a: Secure software development practices for generative ai and dual-use foundation models, 2026. URL https://csrc.nist.gov/pubs/sp/800/218/a/final. NIST Special Publication 800-218A (July 2024), which augments the Secure Software Development Framework with practices specific to AI model development across the software lifecycle. Produced in response to Executive Order 14110, it addresses AI model producers, developers building on those models, and acquirers of AI systems, and is designed to be used alongside NIST SP 800-218.

SIST Guide Reference 291. Revised 508 standards and 255 guidelines, 2026. URL https://www.access-board.gov/ict/. Official documentation from the U.S. Access Board on the Revised 508 Standards and 255 Guidelines for information and communication technology accessibility. It

establishes mandatory accessibility requirements for federal agencies and voluntary guidelines for telecommunications manufacturers, covering hardware, software, websites, electronic documents, and support services.

SIST Guide Reference 292. Assessing risks and impacts of ai (aria): Pilot evaluation report, 2026. URL https://www.nist.gov/publications/assessing-risks-and-impacts-ai-aria-pilot-evaluation-report. The ARIA 0.1 pilot evaluation report documents NIST's methodology for systematically assessing AI applications for risks and societal impacts, using a multi-layered evaluation approach across five participating organizations and seven submitted AI applications. The pilot employed three evaluation scenarios and three testing levels: model testing, red teaming, and field testing, supplemented by dialogue annotation, tester questionnaires, and structured measurement trees.

SIST Guide Reference 293. Inventory of nara artificial intelligence (ai) use cases, 2026. URL https://www.archives.gov/ai. The National Archives and Records Administration (NARA) official inventory of its artificial intelligence use cases, documenting 14 projects across deployed, pilot, and planned stages. Deployed efforts include workplace productivity tools, automated tagging for museum experiences, and historical record retrieval, while pilots cover PII detection and redaction, semantic search, and metadata generation, and planned work targets FOIA processing and public search.

SIST Guide Reference 294. M-25-21: Accelerating federal use of ai through innovation, governance, and public trust, 2026. URL https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf. An April 2025 Office of Management and Budget memorandum (M-25-21) directing executive branch agencies on federal use of artificial intelligence. Issued under Executive Order 14179, it instructs agencies to accelerate adoption of AI to improve public services and government efficiency while maintaining safeguards for civil rights, civil liberties, and privacy.

SIST Guide Reference 295. M-25-22: Driving efficient acquisition of artificial intelligence in government, 2026. URL https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-22-Driving-Efficient-Acquisition-of-Artificial-Intelligence-in-Government.pdf. OMB Memorandum M-25-22 (April 3, 2025), Driving Efficient Acquisition of Artificial Intelligence in Government, issued under Executive Order 13960 and related directives. It provides guidance to federal agencies for acquiring effective and trustworthy AI in a timely, cost-effective manner, and rescinds and replaces earlier memorandum M-24-18.

SIST Guide Reference 296. Artificial intelligence risk management framework: Generative artificial intelligence profile, 2026. URL https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf. NIST AI 600-1, the Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, a cross-sectoral companion resource to the NIST AI RMF 1.0 issued pursuant to Executive Order 14110. It identifies risks that are unique to or amplified by generative AI and organizes suggested actions for managing those risks, mapped to the AI RMF functions.

SIST Guide Reference 297. Intelligence community directive 203: Analytic standards, 2026. URL https://www.odni.gov/files/documents/ICD/ICD-203.pdf. Official ODNI Intelligence Community Directive 203 analytic standards source for objectivity, independence, timeliness, alternatives, confidence, sourcing, and accuracy in analytic products.

SIST Guide Reference 298. Intelligence community directives, 2026. URL https://www.odni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives. Official ODNI index for Intelligence Community Directives used to locate current directive source material and preserve directive-context citations.

SIST Guide Reference 299. Model context protocol specification, 2026. URL https://modelcontextprotocol.io/specification. The official Model Context Protocol (MCP) specification, defining an open protocol that standardizes how LLM applications connect to external data sources and tools using JSON-RPC 2.0 messages. It describes the host, client, and server roles and capability negotiation, and the features servers expose (resources, prompts, tools) and clients offer (sampling, roots, elicitation).

SIST Guide Reference 300. Mitre atlas, 2026. URL https://atlas.mitre.org/. MITRE ATLAS knowledge base for adversarial threats to AI systems, used for defensive AI red-team assurance and misuse taxonomy.

SIST Guide Reference 301. The ic osint strategy 2024-2026, 2026. URL https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf. Official Intelligence Community strategy for open-source intelligence governance, integration, source discovery, data, tools, tradecraft, and workforce priorities.

SIST Guide Reference 302. National geospatial-intelligence agency about us, 2026. URL https://www.nga.mil/about/About_Us.html. The official "About Us" page of the National Geospatial-Intelligence Agency (NGA), a U.S. Department of Defense and intelligence community organization. It describes NGA's mission of delivering geospatial intelligence, or GEOINT, to support military operations, policymakers, and first responders, spanning imagery analysis, mapping, geodesy, and navigation safety.

SIST Guide Reference 303. Software security in supply chains, 2026. URL https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software-1. An official NIST page on software supply chain security issued under Executive Order 14028, focused on the Software Bill of Materials as a formal record of software components and their supply chain. It explains the benefits of SBOMs for vulnerability identification and supply-chain transparency, recommends machine-readable formats such as SPDX, CycloneDX, and SWID, and describes foundational, sustaining, and enhancing levels of implementation.

SIST Guide Reference 304. Secure software development framework (ssdf) version 1.1: Recommendations for mitigating the risk of software vulnerabilities, 2026. URL https://csrc.nist.gov/pubs/sp/800/218/final. NIST SP 800-218, the Secure Software Development Framework Version 1.1 published in February 2022, establishes a set of high-level practices for integrating security into software development lifecycles in order to reduce vulnerabilities in released software, mitigate the impact of exploited vulnerabilities, and address root causes to prevent recurrences.

SIST Guide Reference 305. Devsecops, 2026. URL https://www.nccoe.nist.gov/devsecops. Official NIST NCCoE DevSecOps project page for software factory, secure pipeline, and continuous authorization source support.

SIST Guide Reference 306. Artificial intelligence, 2026. URL https://www.cisa.gov/ai. Official CISA Artificial Intelligence page for AI security, safety, resilience, and critical-infrastructure governance source support.

SIST Guide Reference 307. Ics recommended practices, 2026. URL https://www.cisa.gov/ics/Recommended-Practices. Official CISA Industrial Control Systems recommended practices page for defensive ICS/OT safety, resilience, and incident-preparation guidance.

SIST Guide Reference 308. Preparing for and mitigating foreign influence operations targeting critical infrastructure, 2026. URL https://www.cisa.gov/resources-tools/resources/cisa-insights-preparing-and-mitigating-foreign-influence-operations-targeting-critical. An archived CISA publication, "CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure," providing guidance on the threat that foreign influence campaigns pose to U.S. critical infrastructure.

SIST Guide Reference 309. Stix version 2.1, 2026. URL https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html. An OASIS standard specification defining STIX (Structured Threat Information Expression), a language for exchanging cyber threat intelligence in a standardized, machine-readable form. It establishes a graph-based model with STIX Domain Objects, Cyber-observable Objects, and Relationship Objects, plus meta objects, bundles, and a patterning language for detection.

SIST Guide Reference 310. Taxii version 2.1, 2026. URL https://docs.oasis-open.org/cti/taxii/v2.1/taxii-v2.1.html. The OASIS Standard specification for TAXII (Trusted Automated Exchange of Intelligence Information) Version 2.1, published in 2021 by the OASIS Cyber Threat Intelligence Technical Committee. It defines a RESTful, HTTPS-based API protocol for sharing cyber threat intelligence between organizations, supporting two communication models: Collections (request-response) and Channels (publish-subscribe).

SIST Guide Reference 311. Countering information threats, 2026. URL https://www.nato.int/cps/en/natohq/topics_219728.htm. An official NATO topic page describing the Alliance's approach to countering information threats, defined as intentional, manipulative, and coordinated activities by state and non-state actors including disinformation and propaganda. It explains why such threats matter for democratic processes and institutional trust, and outlines a four-part framework of understanding, preventing, containing, and recovering.

SIST Guide Reference 312. Guide on the use of agentic artificial intelligence, 2026. URL https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/guide-use-agentic-artificial-antelligence.html. Official Government of Canada guide for responsible use of agentic AI, used for public-sector agent governance and accountability source support.

Intelligence Advanced Research Projects Activity. Aggregative contingent estimation, 2010. URL https://www.iarpa.gov/research-programs/ace. Official IARPA ACE program page on eliciting, weighting, and combining probabilistic judgments to improve intelligence forecasts. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: forecasting_calibration_evidence. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: IARPA program page, solicitation status, related-publication links, or archived program metadata changes. Verification method: direct_official_page_review. Claim scope: Supports bounded claims about government-sponsored probabilistic forecasting, elicitation, weighting, aggregation, and empirical testing against real events. Stakeholder role: forecasting instructor; curriculum designer; evaluation lead. Assurance use: Connects SAT lessons to calibration and aggregation evidence without claiming autonomous forecasting judgment. Rights dimension: public IARPA program metadata used for education and source-backed synthesis. Direct IARPA program page verified live 2026-06-15; used for program objectives and forecasting-evidence context, not as an AGEINT performance claim.

Intelligence Advanced Research Projects Activity. Rapid explanation, analysis and sourcing online, 2023. URL https://www.iarpa.gov/research-programs/reason. Official IARPA REASON program page on analyst-in-the-loop evidence and reasoning support for draft analytic reports. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: agentic_analytic_assistance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: IARPA program page, BAA status, technical description, or evaluation language changes. Verification method: direct_official_page_review. Claim scope: Supports bounded claims that AI-enabled reasoning systems can assist evidence discovery and reasoning review while retaining analyst responsibility. Stakeholder role: analytic method designer; AI governance reviewer; curriculum designer. Assurance use: Constrains AI/SAT automation prose away from autonomous strategic judgment, targeting, or report replacement. Rights dimension: public IARPA program metadata used for education and governance review. Direct IARPA program page verified live 2026-06-15; used for bounded analyst-assistance context and explicit non-replacement language.

U.S. General Services Administration. Ai guide for government, 2026. URL https://ai.gov/. Official U.S. government AI resource hub for agency adoption, responsible use, policy references, and public-sector implementation support. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: public_sector_agentic_ai. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: federal AI guidance, agency practice, resource hub, or policy source changes. Verification method: direct_official_page_review. Claim scope: public-sector adoption, agency AI governance, and responsible implementation references. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Central Intelligence Agency. A tradecraft primer: Structured analytic techniques for improving intelligence analysis, 2009. URL https://www.cia.gov/resources/csi/static/Tradecraft-Primer-apr09.pdf. Official structured analytic techniques primer for bias checks, alternatives, and warning analysis. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: analytic_tradecraft. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Central Intelligence Agency. Center for the study of intelligence, 2026a. URL https://www.cia.gov/resources/csi/. Official CSI landing page for Studies in Intelligence, declassified professional reflection, analytic history, and institutional learning. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: historical_declassified_sources. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Defense Advanced Research Projects Agency. Active social engineering defense, 2017a. URL https://www.darpa.mil/research/programs/active-social-engineering-defense. DARPA public program page for Active Social Engineering Defense, used as official defensive context for social-engineering resilience and automation-risk caveats. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: cyber_threat_intelligence. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: DARPA program page, program status, public description, or defensive social-engineering literature materially changes. Verification method: direct_official_page_review. Claim scope: Supports public program-level framing for active social engineering defense; AGEINT uses it for defensive concept boundaries, not for social-engineering operations. Stakeholder role: cyber defender, instructor, social-engineering defense reviewer. Assurance use: social-engineering defense boundary, adversarial-interaction ethics review, and cyber-resilience classroom caveats. Rights dimension: defensive security, consent, transparency, privacy, and protection from manipulation. Direct DARPA source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Defense Advanced Research Projects Agency. Intrinsic cognitive security (ics), 2024a. URL https://www.darpa.mil/research/programs/intrinsic-cognitive-security. DARPA Intrinsic Cognitive Security (ICS) program applying probabilistic formal methods to guarantee mixed-reality system designs mitigate cognitive attacks; CAMP knowledgebase analog to MITRE CAPEC. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: assurance_evaluation_evidence. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: DARPA ICS program scope, formal-methods approach, cognitive-attack taxonomy, or CAMP knowledgebase publication changes. Verification method: direct_official_page_review. Claim scope: intrinsic cognitive security, probabilistic formal methods, cognitive-attack taxonomy for mixed-reality systems, and mathematical mitigation guarantees. Stakeholder role: assurance evaluator, formal-methods reviewer, instructor, system steward, and learner. Assurance use: formal-methods assurance evidence, cognitive-attack mitigation catalogue, and probabilistic-guarantee review for mixed-reality system design. Rights dimension: safety, cognitive integrity, perceptual security, accountable system design, and verifiable assurance. Direct source URL verified live (HTTP 200, on-topic DARPA ICS program page) for AGEINT curriculum use.

Defense Intelligence Agency. Dia instruction 5400.001: Privacy and civil liberties program, 2014. URL https://www.dia.mil/Portals/110/Documents/FOIA/All%20PDFs/DIA-Instructions/DIAI_5400_001.pdf. DIA public instruction for privacy and civil-liberties responsibilities, complaints, records, and safeguards. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: rights_impact_privacy. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: DIA instruction URL, release status, or public policy text materially changes. Verification method: browser_fetch_official_pdf_review. Claim scope: privacy and civil-liberties governance support for legal/ethical review modules. Stakeholder role: privacy reviewer, analyst, instructor. Assurance use: anchors rights-impact review language in an official DIA public instruction. Rights dimension: public instruction used for privacy and civil-liberties education. Direct URL verified on 2026-06-14 through browser fetch because dia.mil returned 403 to plain curl; fetched PDF content matched DIAI 5400.001.

Defense Intelligence Agency. Dia style manual for intelligence production, 2015. URL https://www.dia.mil/Portals/110/Documents/FOIA/All%20PDFs/DIA-Instructions/DIA_Style_Manual_for_Intelligence_Production.pdf. DIA public FOIA release for intelligence-production style, terminology, formatting, and writing consistency. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: intelligence_writing_and_review. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: DIA FOIA URL, style manual version, or public release status changes. Verification method: browser_fetch_official_pdf_review. Claim scope: intelligence-production writing and style support for manuscript clarity and table/heading discipline. Stakeholder role: author, editor, reviewer. Assurance use: supports AGEINT writing conventions and source-backed manuscript-polish gates. Rights dimension: public FOIA release used for education and writing review. Direct URL verified on 2026-06-14 through browser fetch because dia.mil returned 403 to plain curl; fetched PDF metadata matched the DIA Style Manual.

Defense Intelligence Agency. A tradecraft primer: Basic structured analytic techniques, 2016. URL https://www.dia.mil/FOIA/FOIA-Electronic-Reading-Room/FileId/161442/. Defense intelligence structured-analysis primer for classroom analytic exercises. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: analytic_tradecraft. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Defense Intelligence Agency. Defense osint strategy 2024-2028, 2024b. URL https://www.dia.mil/Portals/110/Documents/OSINT-Strategy.pdf. DIA strategy for professionalizing and unifying Defense OSINT collection and reporting in public governance terms. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: defense_osint_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: DIA strategy URL, public release version, or Defense OSINT policy text materially changes. Verification method: browser_fetch_official_pdf_review. Claim scope: public OSINT governance and professionalization support, not collection procedure or live targeting guidance. Stakeholder role: OSINT analyst, instructor, reviewer. Assurance use: anchors OSINT modules to official public Defense governance and source-quality discipline. Rights dimension: public strategy used for education and lawful-source governance. Direct URL verified on 2026-06-14 through browser fetch because dia.mil returned 403 to plain curl; fetched PDF content matched the Defense OSINT Strategy.

National Geospatial-Intelligence Agency. Geoint basic doctrine publication 1, 2017b. URL https://www.nga.mil/assets/files/170901-038_GEOINT_Basic_Doctrine_Pub_1.pdf. NGA doctrine source for GEOINT definitions, mission context, and professional geospatial intelligence framing. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: geoint_professional_doctrine. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: NGA doctrine URL, publication version, or public doctrine text materially changes. Verification method: curl_http_200_pdf_review. Claim scope: GEOINT doctrine and geospatial-intelligence framing support. Stakeholder role: GEOINT analyst, instructor, reviewer. Assurance use: anchors GEOINT modules to official doctrine rather than broad imagery claims. Rights dimension: public doctrine used for education and source-provenance review. Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from nga.mil.

National Geospatial-Intelligence Agency. Nga pub 1.0: Geoint basic doctrine (2018), 2018. URL https://irp.fas.org/agency/nga/doctrine-2018.pdf. Verified official primary source for geoint_doctrine; routed to GEOINT doctrine; NGA mission; GEOINT principles and definitions. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: geoint_doctrine. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for geoint_doctrine materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of geoint_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that geoint_doctrine claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_nga_geoint_pub1_doctrine_2018 retained.

National Geospatial-Intelligence Agency. Nga releases new data strategy to navigate digital, geoint revolution, 2021. URL https://www.nga.mil/news/NGA_releases_new_data_strategy_to_navigate_digital.html. NGA public release on data strategy, geospatial data management, and digital transformation in GEOINT. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: geoint_data_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: NGA page content, data strategy version, or public URL materially changes. Verification method: curl_http_200_html_review. Claim scope: GEOINT data-governance and digital-transformation context for modular source substrate claims. Stakeholder role: GEOINT data steward, analyst, reviewer. Assurance use: supports data-lineage and GEOINT-source governance language. Rights dimension: public release used for education and data-governance framing. Direct URL verified on 2026-06-14 with curl HTTP 200 and text/html content from nga.mil.

National Geospatial-Intelligence Agency. Geoint artificial intelligence, 2026b. URL https://www.nga.mil/news/GEOINT_Artificial_Intelligence_.html. Official NGA source on GEOINT AI, data quality, model performance, interoperability, analyst interaction, and standards leadership. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: osint_geoint. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Geospatial-Intelligence Agency. Nga strategy, 2026c. URL https://www.nga.mil/about/NGA_Strategy.html. Official NGA strategy anchor for GEOINT readiness, warning, partnership resilience, resource stewardship, and AI integration. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: osint_geoint. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Security Agency. Security design considerations for ai-driven automation leveraging mcp, 2025. URL https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4496698/nsa-releases-security-design-considerations-for-ai-driven-automation-leveraging/. Official NSA security guidance for Model Context Protocol automation. Checked as of 2026-05-21. Citation role: source_quality_anchor. Source lane: source_quality_spine. Source tier: source_quality_anchor. Refresh cadence: semiannual. Refresh trigger: source version, legal status, standard revision, or official guidance changes. Verification method: direct_source_url_review. Claim scope: baseline source-quality guardrail for generated AGEINT curriculum claims. Stakeholder role: curriculum maintainer, instructor, reviewer, and learner. Assurance use: source-quality triangulation and claim-boundary review. Rights dimension: source transparency, accountability, and evidence traceability. Directly verified official NSA source URL.

National Security Agency. About nsa mission, 2026d. URL https://www.nsa.gov/about/. NSA public mission page for SIGINT and cybersecurity mission context. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: ic_public_transparency. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: NSA public mission page content or URL materially changes. Verification method: browser_fetch_official_html_review. Claim scope: public mission context for SIGINT/cybersecurity orientation. Stakeholder role: learner, instructor, reviewer. Assurance use: anchors public NSA mission descriptions to the official page. Rights dimension: public education page used for orientation and governance framing. Direct URL verified on 2026-06-14 through browser fetch because nsa.gov returned 403 to plain curl; fetched HTML title and content matched the NSA mission page.

National Security Agency. Nsa joins the asd's acsc and others to release guidance on agentic artificial intelligence systems, 2026e. URL https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4475134/nsa-joins-the-asds-acsc-and-others-to-release-guidance-on-agentic-artificial-in/. NSA public release announcing joint guidance on careful adoption of agentic AI services. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: agentic_ai_security_governance. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: NSA press release, linked guidance, or public agentic AI adoption posture materially changes. Verification method: browser_fetch_official_html_review. Claim scope: agentic AI adoption and security-governance context, not an AGEINT benchmark. Stakeholder role: AI security reviewer, system owner, instructor. Assurance use: supports agentic AI safety-boundary and adoption-gate language. Rights dimension: public cybersecurity release used for defensive AI-governance education. Direct URL verified on 2026-06-14 through browser fetch because nsa.gov returned 403 to plain curl; fetched HTML title and content matched the agentic AI services release.

National Security Agency. Nsa cybersecurity advisories and guidance, 2026f. URL https://www.nsa.gov/press-room/cybersecurity-advisories-guidance/. NSA public index for cybersecurity advisories, information sheets, technical reports, and operational risk notices. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: cyber_defense_guidance_index. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: NSA guidance index structure, source URL, or public guidance inventory materially changes. Verification method: browser_fetch_official_html_review. Claim scope: defensive cyber guidance index support for source routing and refresh duties. Stakeholder role: cyber analyst, instructor, reviewer. Assurance use: supports defensive CTI source routing without citing exploit instructions. Rights dimension: public guidance index used for defensive education and source-refresh planning. Direct URL verified on 2026-06-14 through browser fetch because nsa.gov returned 403 to plain curl; fetched HTML title and content matched the advisories and guidance page.

National Security Agency. Foreign intelligence surveillance act, 2026g. URL https://www.nsa.gov/Signals-Intelligence/FISA/. Official NSA public explanation of FISA oversight for signals intelligence collection governed by statutory and court-authorized controls. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: legal_oversight. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Security Agency. Nsa historical releases, 2026h. URL https://www.nsa.gov/helpful-links/nsa-foia/declassification-transparency-initiatives/historical-releases/. Official declassified historical-release library for cryptologic history, SIGINT history, COMSEC, oral histories, and historical cases. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: historical_declassified_sources. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Security Agency. Model context protocol (mcp): Security design considerations for organizations, 2026i. URL https://www.nsa.gov/Portals/75/documents/Cybersecurity/CSI_MCP_SECURITY.pdf. NSA cybersecurity information sheet on MCP security design considerations for organizations adopting MCP-based AI toolchains. Checked as of 2026-06-11. Citation role: curriculum_anchor. Source lane: secure_release_change_control. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: NSA MCP security guidance, MCP protocol security profile, implementation vulnerability guidance, or secure-adoption recommendations change. Verification method: direct_official_pdf_review. Claim scope: Official cybersecurity information sheet on Model Context Protocol security design considerations, deliberate controls beyond protocol suggestions, and secure adoption safeguards for MCP implementations. Stakeholder role: security architect, release reviewer, agent-platform engineer, procurement assessor, instructor, and learner. Assurance use: MCP security design review, implementation threat model, privilege boundary checklist, reverse-proxy and sandboxing control discussion, and secure-release gate evidence. Rights dimension: security, credential protection, least privilege, supply-chain integrity, sandboxing, auditability, and harm prevention. Direct NSA PDF URL verified live 2026-06-11; guidance frames MCP security adoption controls and recommendations for organizations.

National Security Agency. Tempest: A signal problem (nsa declassified), n.d. URL https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/cryptologic-spectrum/tempest.pdf. Verified official primary source for sigint_emanations_intelligence; routed to SIGINT fundamentals; emanations intelligence; EMSEC/TEMPEST history. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: sigint_emanations_intelligence. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for sigint_emanations_intelligence materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of sigint_emanations_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that sigint_emanations_intelligence claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_nsa_tempest_signal_problem retained.

Nikolas K. G. Artner Alexandru Marcoci, Kristian J. Hammond and Jeff Jonas. Better together: Reliable application of the post-9/11 and post-iraq us intelligence tradecraft standards requires collective analysis, 2019. URL https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2018.02634/full. Peer-reviewed study showing poor individual reliability but stronger aggregated reliability when raters apply tradecraft standards to intelligence reports. Checked as of 2026-06-11. Citation role: curriculum_anchor. Source lane: sat_evaluation_evidence. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: Refresh if journal metadata, correction, or retraction status changes. Verification method: open_article_review. Claim scope: Supports claims about rater reliability limits and value of collective review for tradecraft standards. Stakeholder role: curriculum designer; quality reviewer; analytic standards trainer. Assurance use: Grounds reviewer calibration, aggregate judgment, and quality-control lessons. Rights dimension: open-access scholarly article; cite DOI/journal source. Frontiers open article verified live 2026-06-11; use for tradecraft-rating reliability and collective review claims.

Cloud Security Alliance. Introducing cognitive degradation resilience (cdr): A framework for safeguarding agentic ai systems from systemic collapse, 2025a. URL https://cloudsecurityalliance.org/blog/2025/11/10/introducing-cognitive-degradation-resilience-cdr-a-framework-for-safeguarding-agentic-ai-systems-from-systemic-collapse. CSA Cognitive Degradation Resilience (CDR) framework defining a six-stage degradation cascade for agentic AI networks and seven QSAF-BC controls; treated as a defensive evidence-bounded governance anchor. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: agent_incident_response. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: CSA CDR framework, degradation-stage model, QSAF-BC controls, health-probe guidance, or agentic-AI resilience publication changes. Verification method: direct_official_page_review. Claim scope: cognitive degradation resilience, six-stage agent degradation cascade, health probes, starvation monitors, and QSAF-BC controls for agentic AI. Stakeholder role: AI incident lead, resilience reviewer, instructor, system steward, and learner. Assurance use: agent degradation health probes, six-stage drift monitoring, QSAF-BC control mapping, and systemic-collapse incident review. Rights dimension: safety, reliability, operational resilience, accountable monitoring, and harm prevention. Direct source URL verified live (HTTP 200, on-topic CSA CDR framework) for AGEINT curriculum use.

Cloud Security Alliance. Agentic ai threat modeling framework: Maestro, 2025b. URL https://cloudsecurityalliance.org/blog/2025/02/06/agentic-ai-threat-modeling-framework-maestro. CSA MAESTRO seven-layer threat-modeling framework for the full agentic AI stack from foundation model through agent ecosystem, including the vertical security/compliance layer. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: ai_red_team_assurance. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: CSA MAESTRO framework, seven-layer model,

per-layer mitigation guidance, or agentic-AI threat-modeling publication changes. Verification method: direct_official_page_review. Claim scope: MAESTRO seven-layer agentic threat model, per-layer threats and mitigations, cross-layer vulnerabilities, and security-compliance layer monitoring. Stakeholder role: threat modeler, red-team reviewer, instructor, system steward, and learner. Assurance use: seven-layer threat-model worksheet, cross-layer mitigation map, security-agent self-audit, and agentic threat-modeling review. Rights dimension: security, accountability, transparency, supply-chain integrity, and trustworthy AI assurance. Direct source URL verified live (HTTP 200, on-topic CSA MAESTRO framework) for AGEINT curriculum use.

Cloud Security Alliance. Securing autonomous ai agents, 2026. URL https://cloudsecurityalliance.org/artifacts/securing-autonomous-ai-agents. CSA survey on securing autonomous AI agents quantifying the identity-governance gap; readiness percentages treated as ESTIMATE for curriculum discussion. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: procurement_vendor_governance. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: CSA securing-autonomous-AI-agents survey revisions, identity-governance findings, or agent IAM-readiness data updates. Verification method: direct_official_page_review. Claim scope: securing autonomous AI agents, agent identity governance gaps, runtime IAM readiness, and accountable agent-credential management. Stakeholder role: identity governance lead, procurement assessor, instructor, system steward, and learner. Assurance use: agent identity-governance gap review, IAM-readiness assessment, non-human identity inventory, and procurement assurance checklist. Rights dimension: security, accountability, least-privilege governance, auditability, and operational resilience. Direct source URL verified live (HTTP 200, on-topic CSA securing-autonomous-AI-agents artifact) for AGEINT curriculum use.

& Gordievsky Oleg. Andrew, Christopher. Kgb: The inside story, 1990. URL https://archive.org/details/kgbinsidestoryof0000andr_j8b6. Verified scholarly book metadata source for intelligence_history_soviet; routed to Historical Intelligence Services (Soviet/Russian); KGB organizational doctrine and operations overview. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: intelligence_history_soviet. Source tier: scholarly_book_metadata. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for intelligence_history_soviet materially changes. Verification method: direct_publisher_or_catalog_record_review. Claim scope: Supports bounded AGEINT discussion of intelligence_history_soviet and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that intelligence_history_soviet claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_andrew_gordievsky_1990_kgb_inside_story retained.

& Mitrokhin Vasili. Andrew, Christopher. The sword and the shield, 1999. URL https://archive.org/details/swordshieldmitro0000andr_q5i4. Verified scholarly book metadata source for intelligence_history_soviet; routed to Historical Intelligence Services (Soviet/Russian); primary-source archival history of KGB. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: intelligence_history_soviet. Source tier: scholarly_book_metadata. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for intelligence_history_soviet materially changes. Verification method: direct_publisher_or_catalog_record_review. Claim scope: Supports bounded AGEINT discussion of intelligence_history_soviet and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that intelligence_history_soviet claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_andrew_mitrokhin_1999_sword_shield retained.

Christopher. Andrew. The defence of the realm, 2009. URL https://archive.org/details/defenceofrealmau0000andr_p5s9. Verified scholarly book metadata source for intelligence_history_british_allied; routed to Historical Intelligence Services (British/Allied); institutional history of domestic security intelligence. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: intelligence_history_british_allied. Source tier: scholarly_book_metadata. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for intelligence_history_british_allied materially changes. Verification method: direct_publisher_or_catalog_record_review. Claim scope: Supports bounded AGEINT discussion of intelligence_history_british_allied and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that intelligence_history_british_allied claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_andrew_2009_defend_realm retained.

Anthropic. Building effective ai agents, 2024. URL https://www.anthropic.com/research/building-effective-agents. Anthropic research guide establishing the canonical workflows-versus-agents taxonomy and composable agentic patterns (prompt chaining, routing, parallelization, orchestrator-workers, evaluator-optimizer). Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: agent_interoperability_standards. Source tier: frontier_lab_research. Refresh cadence: semiannual. Refresh trigger: Anthropic Building Effective Agents updates, revised pattern taxonomy, or successor agent-architecture guidance changes. Verification method: direct_research_page_review. Claim scope: agentic architecture taxonomy, workflows versus agents, core orchestration patterns, and design principles favoring simplicity and human checkpoints. Direct source URL verified live (HTTP 200, on-topic Anthropic agent-architecture research) for AGEINT curriculum use.

National Archives and Records Administration. Executive order 12333: United states intelligence activities, 1981. URL https://www.archives.gov/federal-register/codification/executive-order/12333.html. Official legal anchor for intelligence authorities, rights-aware collection, analytic competition, oversight, and source-method protection. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: legal_oversight. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Archives and Records Administration. Nara 2025 ai compliance plan, 2025. URL https://www.archives.gov/files/nara-2025-ai-compliance-plan-final-v1-09-18-2025.pdf. NARA plan for AI governance, public trust, audits, records-aware AI use, transparency, and compliance with federal AI policy. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: records_retention_auditability. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: NARA AI compliance plan, records policy, AI use-case inventory, audit, or federal AI governance update. Verification method: direct_official_pdf_review. Claim scope: agency AI compliance planning, records governance, AI use-case oversight, transparency, and auditability evidence. Stakeholder role: records officer, public-sector AI steward, compliance reviewer, instructor, and learner. Assurance use: records-retention and AI compliance audit trail. Rights dimension: public records, transparency, auditability, privacy-by-design, accountability, and public trust. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Archives and Records Administration. Inventory of nara artificial intelligence (ai) use cases, 2026a. URL https://www.archives.gov/ai. Official NARA inventory of current and planned AI use cases, including production, pilot, and planned AI applications tied to records, discovery, FOIA, and archival access. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: records_retention_auditability. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: NARA AI use-case inventory, agency AI use-case disclosure, records policy, or FOIA

workflow changes. Verification method: direct_official_page_review. Claim scope: AI use-case inventory, records-oriented AI auditability, archival access, and public disclosure. Stakeholder role: records officer, public official, instructor, transparency reviewer, and learner. Assurance use: AI use-case inventory review and records-audit trail. Rights dimension: records access, public transparency, privacy, archival integrity, and FOIA accountability. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Archives and Records Administration. Records of the central intelligence agency, 2026b. URL https://www.archives.gov/research/guide-fed-records/groups/263.html. Official NARA guide to CIA Record Group 263, archival provenance, record series, and declassified intelligence research pathways. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: historical_declassified_sources. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Michael J. Ard. Structured analytic techniques: A pragmatic approach, 2024. URL https://www.tandfonline.com/doi/full/10.1080/08850607.2023.2241308. Peer-reviewed critique arguing that SAT evidence is thinner than many tradecraft claims imply and that SATs should not be treated as universal bias remedies. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: sat_evaluation_evidence. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: Refresh if publisher metadata, correction, or retraction status changes. Verification method: crossref_doi_metadata_review. Claim scope: Supports evidence-boundary claims that SATs need qualification and should not be presented as proven universal debiasing tools. Stakeholder role: curriculum designer; analytic standards trainer; evaluation lead. Assurance use: Forces SAT lessons to distinguish transparency aids from demonstrated accuracy improvements. Rights dimension: copyrighted scholarly article; cite DOI metadata and summarize sparingly. DOI metadata verified live 2026-06-15 through Crossref for title, author, and publication year; publisher URL retained because automated publisher retrieval may be rate-limited.

arXiv preprint authors. Agentic ai security: Threats, defenses, evaluation, and open challenges, 2025a. URL https://arxiv.org/abs/2510.23883v2. arXiv survey on agentic AI security providing a comprehensive threat taxonomy, defense catalog, evaluation review, and governance perspectives; vendor statistics within treated as ESTIMATE. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: ai_red_team_assurance. Source tier: scholarly_preprint. Refresh cadence: quarterly. Refresh trigger: New arXiv version of the agentic-AI security survey, revised threat taxonomy, defense catalog, or evaluation-methodology updates. Verification method: direct_scholarly_page_review. Claim scope: agentic AI security threat taxonomy, prompt-injection and protocol threats, defense strategies, evaluation methodologies, and open challenges. Stakeholder role: red-team reviewer, threat modeler, instructor, system steward, and learner. Assurance use: agentic threat-taxonomy crosswalk, defense-catalog review, evaluation-benchmark map, and open-challenge research log. Rights dimension: security, accountability, transparency, and trustworthy AI assurance. Direct source URL verified live (HTTP 200, on-topic arXiv agentic-AI security survey) for AGEINT curriculum use.

arXiv preprint authors. Systems security foundations for agentic computing, 2025b. URL https://arxiv.org/html/2512.01295v1. arXiv analysis framing prompt injection as structurally equivalent to dynamic code loading and arguing for dynamic, context-sensitive privilege management in agentic systems. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: secure_release_change_control. Source tier: scholarly_preprint. Refresh cadence: annual. Refresh trigger: New arXiv version of Systems Security Foundations for Agentic Computing, revised privilege model, or successor agentic-security-foundations research changes. Verification method: direct_scholarly_page_review. Claim scope: systems security for agentic computing, probabilistic trusted computing bases, dynamic privilege, prompt-injection-as-dynamic-code-loading, and information-flow controls. Stakeholder role: security architect, release reviewer, instructor, system steward, and learner. Assurance use: agentic trusted-computing-base review, dynamic-privilege change-control map, instruction-data separation evidence, and release-gate analysis. Rights dimension: security, integrity, least-privilege accountability, and operational resilience. Direct source URL verified live (HTTP 200, on-topic arXiv agentic systems-security paper) for AGEINT curriculum use.

NSA CCCS NCSC-NZ ASD ACSC, CISA and NCSC-UK. Careful adoption of agentic ai services, 2026. URL https://www.cyber.gov.au/business-government/secure-design/artificial-intelligence/careful-adoption-of-agentic-ai-services. Joint government guidance for deploying agentic AI with identity, logging, and progressive controls. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: agentic_ai_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Infocomm Media Development Authority. Model ai governance framework for agentic ai, 2026. URL https://www.imda.gov.sg/-/media/imda/files/about/emerging-tech-and-research/artificial-intelligence/mgf-for-agentic-ai.pdf. Government framework focused on agentic AI delegation, controls, and safe deployment. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: agentic_ai_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

World Bank. Govtech: Putting people first, 2026. URL https://www.worldbank.org/en/programs/govtech. Official World Bank GovTech program source for digital public infrastructure, citizen engagement, core systems, and public-sector modernization. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: public_sector_agentic_ai. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: GovTech Maturity Index, program priority, case repository, or public-sector digital update. Verification method: direct_official_page_review. Claim scope: government digital transformation, AI-in-government context, and public service accountability. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Alan Barnes and David R. Mandel. Accuracy of forecasts in strategic intelligence, 2014. URL https://www.pnas.org/doi/10.1073/pnas.1406138111. Peer-reviewed PNAS study of strategic-intelligence forecast accuracy, calibration, discrimination, and probability-language behavior. Checked as of 2026-06-11. Citation role: curriculum_anchor. Source lane: forecasting_calibration_evidence. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: Refresh if publisher metadata, correction, or retraction status changes. Verification method: publisher_and_pubmed_metadata_review. Claim scope: Supports bounded claims about strategic-intelligence forecast accuracy, calibration, discrimination, and underconfidence. Stakeholder role: curriculum designer; forecasting instructor; evaluation lead. Assurance use: Links probability language and calibration exercises to empirical forecasting evidence. Rights dimension: copyrighted scholarly article; cite metadata and avoid extended quotation. PNAS DOI/publisher page and PubMed metadata verified live 2026-06-11; use for forecast-calibration claims.

Richard K. Betts. Analysis, war, and decision: Why intelligence failures are inevitable, 1978. URL https://www.cambridge.org/core/journals/world-politics/article/abs/analysis-war-and-decision-why-intelligence-failures-are-inevitable/FB02E0C3A2E0EC5567C678044B3EB828. Classic peer-reviewed failure-theory article on the interaction of analysis, decision, leadership psychology, and policy uptake. Checked as of 2026-06-11. Citation role: curriculum_anchor. Source lane: intelligence_failure_postmortem. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: Refresh if publisher metadata or DOI record changes. Verification method: publisher_record_review. Claim scope: Supports claims that intelligence failure often emerges from analysis-decision interaction and cannot be reduced to missing technique alone. Stakeholder role: curriculum designer; intelligence history instructor; governance reviewer. Assurance use: Keeps failure lessons attentive to policy uptake, incentives, and organizational learning. Rights dimension: copyrighted scholarly article metadata; cite and summarize sparingly. Cambridge Core publisher page verified live 2026-06-11; use for failure-theory context, not fatalistic claims that improvement is impossible.

J. Biden. Executive order 14028 on improving the nation's cybersecurity, 2021. URL https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity. Verified official primary source for supply_chain_intelligence_attacks; routed to Supply Chain Intelligence Attacks; Cyber Intelligence Fundamentals; ICS/OT Security. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: supply_chain_intelligence_attacks. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for supply_chain_intelligence_attacks materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of supply_chain_intelligence_attacks and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that supply_chain_intelligence_attacks claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_whitehouse_eo_14028 retained; stale or indirect proposal URL replaced with direct source record.

European Data Protection Board. Endorsed wp29 guidelines, 2018. URL https://www.edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines_en. EDPB list of endorsed WP29 GDPR guidelines, including DPIA guidance for processing likely to result in a high risk. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: rights_impact_privacy. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: EDPB guideline endorsement, supersession, or GDPR guidance page changes. Verification method: direct_official_page_review. Claim scope: DPIA source verification, privacy-governance references, and GDPR evidence traceability. Stakeholder role: privacy officer, legal reviewer, instructor, and learner. Assurance use: verified DPIA reference and source-refresh evidence. Rights dimension: privacy, data protection, transparency, and accountable processing. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

European Data Protection Board. What is a data protection impact assessment and when is this mandatory?, 2026. URL https://www.edpb.europa.eu/sme-data-protection-guide/faq-frequently-asked-questions/answer/what-data-protection-impact_en. EDPB data-protection guide entry defining DPIA use for planned processing, high-risk processing, automated evaluation, sensitive data, and systematic monitoring. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: rights_impact_privacy. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: EDPB DPIA guidance, GDPR interpretation, SME guide, or high-risk processing examples change. Verification method: direct_official_page_review. Claim scope: DPIA triage, privacy impact worksheets, high-risk processing criteria, and safeguard evidence. Stakeholder role: data controller, data subject, instructor, reviewer, and privacy officer. Assurance use: DPIA trigger worksheet and mitigation record. Rights dimension: privacy, data protection, automated-decision safeguards, and redress. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

United States Access Board. Revised 508 standards and 255 guidelines, 2017. URL https://www.access-board.gov/ict/. Official ICT accessibility standards for federal information and communication technology, including procurement, development, maintenance, use, exceptions, and documentation. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: learner_support_accommodations. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: federal ICT accessibility standard, accessibility rule, exception, or documentation requirement changes. Verification method: direct_official_page_review. Claim scope: learner support plans, accessibility exception documentation, alternative means, and artifact remediation. Stakeholder role: learner, instructor, accessibility reviewer, procurement reviewer, and public-service owner. Assurance use: accommodation plan, accessibility remediation log, and alternative-means decision. Rights dimension: accessibility, equal participation, public-service access, and reasonable accommodation. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Smith A. Bartol N.-Winkler K. Holbrook A. & Fallon M. Boyens, J. Cybersecurity supply chain risk management practices for systems and organizations (nist sp 800-161 rev. 1), 2022. URL https://csrc.nist.gov/pubs/sp/800/161/r1/final. Verified official primary source for supply_chain_intelligence_attacks; routed to Supply Chain Intelligence Attacks; ICS/OT Security; Threat Intelligence Sharing. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: supply_chain_intelligence_attacks. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for supply_chain_intelligence_attacks materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of supply_chain_intelligence_attacks and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that supply_chain_intelligence_attacks claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_nist_sp_800_161r1_scrm retained.

Kleinman S. M. Oleszkiewicz-S. & Meissner C. A. Brimbal, L. Developing rapport and trust in the interrogative context: An empirically supported alternative, 2020. URL https://academic.oup.com/book/40539/chapter/347867388. An Oxford volume chapter reviewing the empirical and ethical case for rapport- and trust-based interrogation as an alternative to customary coercive practices, grounding the contrast between rapport-based and coercive elicitation and the ethics/consent governance that distinguishes them. Checked as of 2026-06-08. Citation role: curriculum_anchor. Source lane: counterintelligence_source_integrity. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: source URL, DOI, edition/standard version, or claim scope materially changes. Verification method: direct_source_url_review. Claim scope: Backs the AGEINT contrast between rapport-based and coercive elicitation and its ethics/consent governance framing. Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.

Stephen J. Artner; Richard S. Girven; James B. Bruce. Assessing the value of structured analytic techniques in the u.s. intelligence community, 2016. URL https://www.rand.org/content/dam/rand/pubs/research_reports/RR1400/RR1408/RAND_RR1408.pdf. RAND report on the difficulty of measuring SAT value and the need for systematic evaluation before strong effectiveness claims. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: sat_evaluation_evidence. Source tier: policy_research_report. Refresh cadence: annual. Refresh trigger: Refresh if RAND publishes a newer SAT evaluation synthesis or corrects report metadata. Verification method: publisher_record_and_pdf_url_review. Claim scope: Supports claims that SAT effectiveness evidence is limited and requires systematic evaluation. Stakeholder role: curriculum designer; evaluation lead; analyst supervisor. Assurance use: Prevents overclaiming that SATs generally cure bias or guarantee accuracy. Rights dimension: RAND copyrighted report; cite metadata and summarize sparingly. RAND report metadata and PDF URL verified again on 2026-06-15 from the RAND publication record and direct PDF URL; use for evaluation-limit claims and evidence-boundary framing.

R. Burkett. An alternative framework for agent recruitment: From mice to rascls, 2013. URL https://www.cia.gov/resources/csi/studies-in-intelligence/volume-57-no-1/an-alternative-framework-for-agent-recruitment-from-mice-to-rascls/. A CIA Studies in Intelligence analyst essay arguing that the traditional MICE recruitment-motivation model (Money, Ideology, Compromise, Ego) is better understood through Cialdini's influence principles reframed as RASCLS (Reciprocation, Authority, Scarcity, Commitment/Consistency, Liking, Social Proof), grounding the historical and conceptual lineage of HUMINT recruitment frameworks. Checked as of 2026-06-08. Citation role: curriculum_anchor. Source lane: counterintelligence_source_integrity. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, DOI, edition/standard version, or claim scope materially changes. Verification method: direct_source_url_review. Claim scope: Backs the MICE-to-RASCLS recruitment-motivation framework with the original official CIA source, supplementing a secondary training-book treatment. Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.

William N. Caballero and Phillip R. Jenkins. On large language models in national security applications, 2024. URL https://arxiv.org/abs/2407.03453. arXiv preprint on LLMs in national-security applications, useful for classroom risk framing because it explicitly treats LLMs as support tools needing safeguards rather than strategic decision-makers. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: ai_enabled_analysis_boundary. Source tier: scholarly_preprint. Refresh cadence: semiannual. Refresh trigger: arXiv version, DOI record, national-security LLM literature, or risk framing materially changes. Verification method: direct_arxiv_page_review. Claim scope: Supports bounded discussion of LLM assistance, hallucination, privacy, adversarial vulnerability, and supporting-role limits in national-security applications; not evidence for autonomous strategic judgment. Stakeholder role: AI governance reviewer, analyst, instructor, red-team reviewer. Assurance use: LLM assistance risk review, human-judgment boundary checks, and national-security classroom case framing. Rights dimension: privacy, reliability, human accountability, adversarial robustness, and public trust. Direct arXiv source URL verified on 2026-06-15 with title, authors, abstract, DOI record, and subject metadata visible on the primary page.

Pendergast A. & Betz C. Caltagirone, S. The diamond model of intrusion analysis, 2013. URL https://apps.dtic.mil/sti/pdfs/ADA586960.pdf. Verified professional documentation source for cyber_threat_intelligence; routed to Cyber Intelligence Fundamentals; APT Analysis; Structured Analytic Techniques for Cyber CTI. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: cyber_threat_intelligence. Source tier: professional_documentation. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for cyber_threat_intelligence materially changes. Verification method: direct_source_url_review. Claim scope: Supports bounded AGEINT discussion of cyber_threat_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that cyber_threat_intelligence claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_caltagirone_2013_diamond_model normalized to professional_caltagirone_2013_diamond_model.

CAST. Cast universal design for learning guidelines version 3.0, 2024. URL https://udlguidelines.cast.org/. CAST UDL Guidelines 3.0 source for designing multiple means of engagement, representation, action, expression, and learner agency. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: accessibility_digital_inclusion. Source tier: education_guidance. Refresh cadence: annual. Refresh trigger: UDL guideline version, citation guidance, or inclusive-learning practice changes. Verification method: direct_official_page_review. Claim scope: inclusive curriculum design, learner variability, assessment flexibility, and facilitation review. Stakeholder role: learner, instructor, accommodation reviewer, and curriculum steward. Assurance use: UDL review checklist and inclusive-assessment evidence. Rights dimension: accessibility, inclusion, learner agency, and educational equity. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Center for the Study of Intelligence Central Intelligence Agency. The need for an intelligence literature, 1955. URL https://www.cia.gov/resources/csi/static/Need-for-Intelligence-Literature.pdf. Classic CIA/CSI source for why intelligence practice needs a professional literature and reviewable doctrine. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: intelligence_profession_literature. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: CIA source URL, release status, or public text materially changes. Verification method: curl_http_200_pdf_review. Claim scope: professional-literature and method-governance support for Synthetic Analytic Tradecraft framing. Stakeholder role: method instructor, author, reviewer. Assurance use: anchors claims that AGEINT is an inspectable literature-backed substrate, not a private prompt collection. Rights dimension: public professional literature used for education and review without operational tasking. Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.

Center for the Study of Intelligence Central Intelligence Agency. The ic's struggle to express uncertainty in the 1970s, 1970s. URL https://www.cia.gov/resources/csi/static/ICs-Struggle-to-Express.pdf. CIA/CSI historical source for uncertainty vocabulary, disagreement, and estimative communication problems. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: analytic_uncertainty_language. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: CIA source URL, release status, or public text materially changes. Verification method: curl_http_200_pdf_review. Claim scope: historical uncertainty-communication support and analytic-language caution. Stakeholder role: analyst, reviewer, writing coach. Assurance use: anchors exercises that separate likelihood, confidence, dissent, and caveats. Rights dimension: public professional literature used for education and review without operational tasking. Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.

Center for the Study of Intelligence Central Intelligence Agency. Words of estimative probability, 1993. URL https://www.cia.gov/resources/csi/static/Words-of-Estimative-Probability.pdf. CIA/CSI source for disciplined probability language and the review boundary between estimative wording, evidence, and numeric interpretation. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: analytic_uncertainty_language. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: CIA source URL, release status, or public text materially changes. Verification method: curl_http_200_pdf_review. Claim scope: estimative-language calibration and uncertainty-expression support, not empirical AGEINT benchmark evidence. Stakeholder role: analyst, reviewer, method instructor. Assurance use: checks whether probability words, confidence, and evidence limits remain separated. Rights dimension: public professional literature used for education and review without operational tasking. Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.

Center for the Study of Intelligence Central Intelligence Agency. Sherman kent and the board of national estimates: Collected essays, 1994. URL https://www.cia.gov/resources/csi/static/sherman-kent-and-the-board-of-national-estimates-collected-essays.pdf. CIA/CSI historical professional source for estimative practice, institutional review, and the Board of National Estimates. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: declassified_analytic_history. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: CIA source URL, release status, or public text materially changes. Verification method: curl_http_200_pdf_review. Claim scope: declassified historical support for analytic-profession and estimative-institution lessons. Stakeholder role: historian, analyst, reviewer. Assurance use: keeps historical institutional claims tied to declassified official material. Rights dimension: public declassified history used for education and governance lessons. Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.

Center for the Study of Intelligence Central Intelligence Agency. Cia and the vietnam policymakers: Three episodes 1962-1968, 1998. URL https://www.cia.gov/resources/csi/static/1768c7c6f5560bafdc7c57afc7b0f1d6/CIA-and-the-Vietnam-Policymakers.pdf. CIA/CSI declassified historical source for analyst-policy boundary lessons and historical interpretation limits. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: declassified_analytic_history. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: CIA source URL, release status, or public text materially changes. Verification method: curl_http_200_pdf_review. Claim scope: declassified history support for analyst-policymaker boundary and institutional lessons. Stakeholder role: historian, analyst, policy reviewer. Assurance use: anchors historical case discussion without translating it into current operational procedure. Rights dimension: public declassified history used for education and governance lessons. Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.

Center for the Study of Intelligence Central Intelligence Agency. Psychology of intelligence analysis, 1999. URL https://www.cia.gov/resources/csi/static/Pyschology-of-Intelligence-Analysis.pdf. CIA/CSI public PDF of Richards Heuer's work on cognition, bias, evidence evaluation, and analytic judgment. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: analytic_cognition_and_bias. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: CIA source URL, release status, or public text materially changes. Verification method: curl_http_200_pdf_review. Claim scope: cognitive and analytic-judgment support for bias-aware review, not universal debiasing proof. Stakeholder role: analyst, instructor, reviewer. Assurance use: supports misconception checks and cognitive-bias caveats in topic lessons. Rights dimension:

public professional literature used for education and review without operational tasking. Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov; note retains CIA disclaimer context.

Center for the Study of Intelligence Central Intelligence Agency. Fifty years of studies in intelligence, 2005a. URL https://www.cia.gov/resources/csi/static/Fifty-Years-Studies-Intel.pdf. CIA/CSI reflection on Studies in Intelligence as an official professional literature venue. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: intelligence_profession_literature. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: CIA source URL, release status, or public text materially changes. Verification method: curl_http_200_pdf_review. Claim scope: professional-literature history for manuscript and curriculum-source governance. Stakeholder role: author, reviewer, historian. Assurance use: supports claims about public professional literature as a reviewable source surface. Rights dimension: public professional literature used for education and review without operational tasking. Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.

Center for the Study of Intelligence Central Intelligence Agency. Creation of a national institute for analytic methods, 2005b. URL https://www.cia.gov/resources/csi/static/National-Institute-Analytic-Methods.pdf. CIA/CSI source on analytic-method evaluation, evidence standards, and institutional method development. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: analytic_method_design. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: CIA source URL, release status, or public text materially changes. Verification method: curl_http_200_pdf_review. Claim scope: method-development support for verifier-first analytic substrate design. Stakeholder role: method designer, evaluator, reviewer. Assurance use: anchors method claims to reviewable institutional evaluation needs rather than intuition. Rights dimension: public professional literature used for education and review without operational tasking. Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.

Center for the Study of Intelligence Central Intelligence Agency. When everything is intelligence - nothing is intelligence, 2006. URL https://www.cia.gov/resources/csi/studies-in-intelligence/archives/when-everything-is-intelligence-nothing-is-intelligence/. CIA/CSI article for defining intelligence analysis around uncertainty rather than undifferentiated information processing. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: intelligence_profession_literature. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: CIA article URL, archive status, or public text materially changes. Verification method: curl_http_200_html_review. Claim scope: definition and professional-boundary support for intelligence-analysis framing. Stakeholder role: analyst, instructor, reviewer. Assurance use: helps prevent source availability from being treated as analytic judgment. Rights dimension: public professional literature used for education and review without operational tasking. Direct URL verified on 2026-06-14 with curl HTTP 200 and text/html content from cia.gov.

Center for the Study of Intelligence Central Intelligence Agency. The limits of prediction - or, how i learned to stop worrying about black swans and love analysis, 2017. URL https://www.cia.gov/resources/csi/static/Limits-of-Prediction.pdf. CIA/CSI source for prediction limits, forecasting caution, and analytic improvement boundaries. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: forecasting_calibration_evidence. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: CIA source URL, release status, or public text materially changes. Verification method: curl_http_200_pdf_review. Claim scope: prediction-limit and forecasting-caution support, not evidence of AGEINT forecast accuracy. Stakeholder role: analyst, forecaster, reviewer. Assurance use: anchors rejection of overstrong prediction, proof, and benchmark claims. Rights dimension: public professional literature used for education and review without operational tasking. Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.

Center for the Study of Intelligence Central Intelligence Agency. A call for more humility in intelligence analysis, 2018a. URL https://www.cia.gov/resources/csi/static/a-call-for-humility.pdf. CIA/CSI article supporting humility, uncertainty, and limits in analytic judgment. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: analytic_cognition_and_bias. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: CIA source URL, release status, or public text materially changes. Verification method: curl_http_200_pdf_review. Claim scope: analytic-humility support for calibrated claims and challengeable evidence packets. Stakeholder role: analyst, reviewer, instructor. Assurance use: anchors reviewer checklists that ask what evidence does not establish. Rights dimension: public professional literature used for education and review without operational tasking. Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.

Center for the Study of Intelligence Central Intelligence Agency. Developing a taxonomy of intelligence analysis variables, 2018b. URL https://www.cia.gov/resources/csi/static/Developing-a-Taxonomy.pdf. CIA/CSI analytic-methods source for decomposing analysis variables and avoiding one-piece judgment claims. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: analytic_method_design. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: CIA source URL, release status, or public text materially changes. Verification method: curl_http_200_pdf_review. Claim scope: taxonomy and analytic-variable support for source-backed method decomposition. Stakeholder role: method designer, reviewer, instructor. Assurance use: supports modular decomposition of claims, variables, evidence, and uncertainty. Rights dimension: public professional literature used for education and review without operational tasking. Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.

Center for the Study of Intelligence Central Intelligence Agency. Managing the reliability cycle: An alternative approach to thinking about intelligence failure, 2018c. URL https://www.cia.gov/resources/csi/static/Managing-the-Reliability-Cycle.pdf. CIA/CSI source for reliability, intelligence failure, feedback, and institutional learning cycles. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: intelligence_failure_postmortem. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: CIA source URL, release status, or public text materially changes. Verification method: curl_http_200_pdf_review. Claim scope: failure-analysis and reliability-cycle support for reviewer challenge and rollback claims. Stakeholder role: reviewer, red team, instructor. Assurance use: supports negative-control and after-action learning language. Rights dimension: public professional literature used for education and review without operational tasking. Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.

Center for the Study of Intelligence Central Intelligence Agency. Thinking and writing: Cognitive science and intelligence analysis, 2018d. URL https://www.cia.gov/resources/csi/static/9e870ec099fc6192e2e412bee248257e/Thinking-and-Writing.pdf. CIA/CSI source connecting cognitive science, analytic writing, and intelligence-analysis communication. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: intelligence_writing_and_review. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: CIA source URL, release status, or public text materially changes. Verification method: curl_http_200_pdf_review. Claim scope: writing and cognitive-science context for clearer evidence packets and analytic communication. Stakeholder role: author, analyst, reviewer. Assurance use: supports prose gates that demand concrete claims, caveats, and reader-inspectable reasoning. Rights dimension: public professional literature used for education and review without operational tasking. Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.

Center for the Study of Intelligence Central Intelligence Agency. War and chance: Assessing uncertainty in international politics, 2018e. URL https://www.cia.gov/resources/csi/static/Review-War-and-Chance.pdf. CIA/CSI review source for uncertainty, probability expression, and the limits of confident prediction. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: analytic_uncertainty_language. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: CIA source URL, release status, or public text materially changes. Verification method: curl_http_200_pdf_review. Claim scope: uncertainty-language and prediction-limit context for calibrated analytic prose. Stakeholder role: analyst, instructor, reviewer. Assurance use: supports wording that avoids proof, certainty, or overconfident statistical implication. Rights dimension: public professional literature used for education and review without operational tasking. Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.

Center for the Study of Intelligence Central Intelligence Agency. Why bad things happen to good analysts, 2018f. URL https://www.cia.gov/resources/csi/static/Why-Bad-Things-Happen.pdf. CIA/CSI source for analyst error, limits, and institutional conditions around analytic failure. Checked

as of 2026-06-14. Citation role: curriculum_anchor. Source lane: intelligence_failure_postmortem. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: CIA source URL, release status, or public text materially changes. Verification method: curl_http_200_pdf_review. Claim scope: failure-mode support for calibrated reviewer challenge and non-guarantee language. Stakeholder role: analyst, reviewer, instructor. Assurance use: supports lessons that distinguish reviewable practice from proof of correctness. Rights dimension: public professional literature used for education and review without operational tasking. Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.

Center for the Study of Intelligence Central Intelligence Agency. The future of analysis, 2019. URL https://www.cia.gov/resources/csi/static/Future-of-Analysis.pdf. CIA/CSI source for future analytic work, data volume, automation, and human analytic structure. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: ai_enabled_analysis_boundary. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: CIA source URL, release status, or public text materially changes. Verification method: curl_http_200_pdf_review. Claim scope: future-analysis context for bounded AI assistance and human analytic structure, not deployed benchmark evidence. Stakeholder role: analyst, AI governance reviewer, instructor. Assurance use: anchors agentic-assistance claims to professional context and limits. Rights dimension: public professional literature used for education and review without operational tasking. Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.

Center for the Study of Intelligence Central Intelligence Agency. Lessons from sable spear: The application of an artificial intelligence methodology to tactical intelligence, 2020. URL https://www.cia.gov/resources/csi/static/ArticleSableSpearExperimentInAI.pdf. CIA/CSI article on an AI-enabled analytic experiment, used as bounded professional context for AI-assisted analysis. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: ai_enabled_analysis_boundary. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: CIA source URL, release status, or public text materially changes. Verification method: curl_http_200_pdf_review. Claim scope: professional-context support for AI-assisted analysis boundaries, not AGEINT benchmark evidence. Stakeholder role: AI governance reviewer, analyst, instructor. Assurance use: supports examples that keep AI assistance reviewable, bounded, and evidence-bounded. Rights dimension: public professional literature used for education and review without operational tasking. Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.

Center for the Study of Intelligence Central Intelligence Agency. Voice of experience: Principles of intelligence analysis, 2021a. URL https://www.cia.gov/resources/csi/static/Article-Principles-of-Intelligence-Analysis-Studies65-4-Dec2021.pdf. CIA/CSI article on foundational elements of intelligence analysis and disciplined analytic practice. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: analytic_method_design. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: CIA source URL, release status, or public text materially changes. Verification method: curl_http_200_pdf_review. Claim scope: professional principle support for source-backed analytic synthesis and reviewer handoff. Stakeholder role: analyst, instructor, reviewer. Assurance use: supports modular practice-language around evidence, assumptions, and judgment. Rights dimension: public professional literature used for education and review without operational tasking. Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.

Center for the Study of Intelligence Central Intelligence Agency. Intelligent analysis: How to defeat uncertainty in high-stakes decisions, 2021b. URL https://www.cia.gov/resources/csi/static/Review_Intelligence_Analysis_in_Uncertainty_Dec_2021.pdf. CIA/CSI review source for uncertainty-management literature and analytic decision support. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: analytic_uncertainty_language. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: CIA source URL, release status, or public text materially changes. Verification method: curl_http_200_pdf_review. Claim scope: uncertainty-management context for bounded analytic-decision support language. Stakeholder role: analyst, reviewer, instructor. Assurance use: supports calibrated uncertainty language without implying AGEINT benchmark results. Rights dimension: public professional literature used for education and review without operational tasking. Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.

Center for the Study of Intelligence Central Intelligence Agency. Agile analysis: Transforming intelligence production through lean startup principles, 2023. URL https://www.cia.gov/resources/csi/static/Article-An-Approach-Agile-Analysis-Sep-2023.pdf. CIA/CSI source for team-based analytic production, iteration, and experimentation boundaries. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: analytic_production_workflow. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: CIA source URL, release status, or public text materially changes. Verification method: curl_http_200_pdf_review. Claim scope: workflow and analytic-production support for iterative, reviewable tradecraft artifacts. Stakeholder role: team lead, analyst, reviewer. Assurance use: anchors modular workflow claims while preserving human review and experiment limits. Rights dimension: public professional literature used for education and review without operational tasking. Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.

Center for the Study of Intelligence Central Intelligence Agency. Applying epistemology to intelligence analysis, 2025a. URL https://www.cia.gov/resources/csi/static/Article-Applying-Epistemology-to-Intelligence-Analysis-Sep-2025.pdf. CIA/CSI source for epistemic framing, objectivity, knowledge claims, and analytic habits of thinking. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: analytic_epistemology. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: CIA source URL, release status, or public text materially changes. Verification method: curl_http_200_pdf_review. Claim scope: epistemic-framing support for calibrated claims and reviewer challengeability. Stakeholder role: analyst, epistemic reviewer, instructor. Assurance use: supports claim-calibration language about what evidence can and cannot establish. Rights dimension: public professional literature used for education and review without operational tasking. Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.

Center for the Study of Intelligence Central Intelligence Agency. Studies in intelligence author's guide 2025: Guidance section only, 2025b. URL https://www.cia.gov/resources/csi/static/Studies-Writers-Guide-2025-Guidance-Section-Only.pdf. CIA/CSI writing-guide source for public professional writing norms, review boundaries, and publication discipline. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: intelligence_writing_and_review. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: CIA guide version, source URL, or public release status changes. Verification method: curl_http_200_pdf_review. Claim scope: professional writing and review-process support for manuscript discipline. Stakeholder role: author, editor, reviewer. Assurance use: supports writing gates that distinguish public professional analysis from agency policy or operational direction. Rights dimension: public professional guidance used for education and manuscript review. Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.

Center for the Study of Intelligence Central Intelligence Agency. Espionage in our ai future, 2026. URL https://www.cia.gov/resources/csi/static/Article-Espionage-in-Our-AI-Future-Studies-70-1-Mar2026.pdf. CIA/CSI 2026 article for AI-era espionage context, source skepticism, and human-review boundaries. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: ai_enabled_analysis_boundary. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: CIA source URL, release status, or public text materially changes. Verification method: curl_http_200_pdf_review. Claim scope: AI-era intelligence context for bounded agentic assistance and counterintelligence caution. Stakeholder role: AI governance reviewer, analyst, counterintelligence instructor. Assurance use: supports safe framing of AI assistance, espionage risk, and reviewer control without operational instructions. Rights dimension: public professional literature used for education and review without operational tasking. Direct URL verified on 2026-06-14 with curl HTTP 200 and application/pdf content from cia.gov.

UK National Cyber Security Centre and international partners. Guidelines for secure ai system development, 2024. URL https://www.ncsc.gov.uk/collection/guidelines-secure-ai-system-development. NCSC Guidelines for secure AI system development for providers of systems that use AI, including systems built from scratch and systems built on top of third-party tools or services. Checked as of 2026-06-06. Citation role: curriculum_anchor. Source lane: secure_release_change_control. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: NCSC secure-AI-development guidance, joint-authority updates, secure-by-design AI controls, supply-chain guidance, or provider responsibility model changes. Verification method:

direct_official_page_review. Claim scope: secure AI system development across design, development, deployment, operation, supply-chain security, and provider-customer responsibility boundaries. Stakeholder role: secure-AI engineer, release reviewer, procurement assessor, instructor, and learner. Assurance use: secure-AI lifecycle review, provider-customer responsibility map, supply-chain checklist, and release-readiness evidence. Rights dimension: security, resilience, accountability, supply-chain integrity, transparency, and harm prevention. Direct source URL verified live (HTTP 200, on-topic NCSC secure-AI-development guidance page) for AGEINT curriculum use.

Pashler H. Vul E. Wixted J. T. & Rohrer D. Cepeda, N. J. Distributed practice in verbal recall tasks, 2006. URL https://www.yorku.ca/ncepeda/publications/CPVWR2006.html. Verified scholarly repository record source for cognitive_performance; routed to Productivity Intelligence & Cognitive Performance (information architecture, spaced repetition); Instructor Capstone/Rubric/Red-Team Pack appendix. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: cognitive_performance. Source tier: scholarly_repository_record. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for cognitive_performance materially changes. Verification method: direct_source_url_review. Claim scope: Supports bounded AGEINT discussion of cognitive_performance and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that cognitive_performance claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_cepeda_2006_spaced_repetition retained.

Supply chain Levels for Software Artifacts Project. Slsa specification, 2026. URL https://slsa.dev/spec/v1.1/. SLSA specification for describing and incrementally improving software supply-chain security, used to ground artifact provenance and release-control claims. Checked as of 2026-06-06. Citation role: curriculum_anchor. Source lane: secure_release_change_control. Source tier: security_standard. Refresh cadence: quarterly. Refresh trigger: SLSA specification version, provenance model, build-level requirement, dependency track, or supply-chain security guarantee changes. Verification method: direct_project_specification_review. Claim scope: supply-chain security levels, build provenance, artifact integrity, dependency risk, and incremental release-control guarantees. Stakeholder role: release engineer, supply-chain reviewer, procurement assessor, instructor, and learner. Assurance use: release-gate provenance checklist, build-integrity assessment, supply-chain risk review, and rollback evidence package. Rights dimension: security, accountability, resilience, transparency, and harm reduction. Direct source URL verified live (HTTP 200, official SLSA v1.1 specification page with on-topic description metadata) for AGEINT curriculum use.

A. Cherepanov. Win32/industroyer: A new threat for industrial control systems, 2017. URL https://web-assets.esetstatic.com/wls/2017/06/Win32_Industroyer.pdf. Verified professional documentation source for historical_ics_incidents; routed to Historical ICS Cyber Incidents; ICS/OT Security; MITRE ATT&CK for ICS. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: historical_ics_incidents. Source tier: professional_documentation. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for historical_ics_incidents materially changes. Verification method: direct_source_url_review. Claim scope: Supports bounded AGEINT discussion of historical_ics_incidents and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that historical_ics_incidents claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_eset_win32_industroyer_2017 normalized to professional_eset_win32_industroyer_2017.

Simon McGregor Christopher L. Buckley, Chang Sub Kim and Anil K. Seth. The free energy principle for action and perception: A mathematical review, 2017. URL https://arxiv.org/abs/1705.09156. arXiv scholarly review that works through the free energy principle and active inference mathematically, including an agent-based model and the assumptions needed for the formal result. Checked as of 2026-06-10. Citation role: curriculum_anchor. Source lane: cognitive_active_inference. Source tier: scholarly_preprint. Refresh cadence: annual. Refresh trigger: arXiv record, DOI record, active-inference review literature, or cited mathematical formulation materially changes. Verification method: direct_scholarly_page_review. Claim scope: Mathematical review of the free energy principle and active inference as a theory of action and perception, including variational free energy, generative models, and explicit modeling assumptions. Stakeholder role: instructor, learner, assurance reviewer, curriculum maintainer, and governance reviewer. Assurance use: active-inference theory review, classroom analogy boundary setting, formal-claim caveat review, and governance handoff evidence. Rights dimension: prevents theory-to-governance overclaiming, separates formal theory from pedagogical analogy, and blocks unsupported autonomous-action claims. Direct arXiv source URL verified live 2026-06-10 with title, authors, submission date, abstract, and DOI metadata matching the cited mathematical review.

Robert B. Cialdini. Influence: The psychology of persuasion (cialdini, 1984), 1984. URL https://books.google.com/books/about/Influence.html?id=mJidPwAACAAJ. Verified scholarly book metadata source for social_engineering_influence_psychology; routed to Social Engineering; Active Measures and Disinformation; Information Warfare and Cognitive Security. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: social_engineering_influence_psychology. Source tier: scholarly_book_metadata. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for social_engineering_influence_psychology materially changes. Verification method: direct_publisher_or_catalog_record_review. Claim scope: Supports bounded AGEINT discussion of social_engineering_influence_psychology and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that social_engineering_influence_psychology claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_cialdini_1984_influence_psychology retained; stale or indirect proposal URL replaced with direct source record.

CISA. Advanced persistent threat compromise of government agencies, critical infrastructure, and private sector organizations (aa20-352a), 2020. URL https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a. Verified official primary source for supply_chain_intelligence_attacks; routed to Supply Chain Intelligence Attacks; Advanced Persistent Threats; Threat Intelligence Sharing. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: supply_chain_intelligence_attacks. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for supply_chain_intelligence_attacks materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of supply_chain_intelligence_attacks and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that supply_chain_intelligence_attacks claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_cisa_aa20_352a_solarwinds retained.

FBI et al. CISA, NSA. Prc state-sponsored actors compromise and maintain persistent access to u.s. critical infrastructure (aa24-038a), 2024. URL https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a. Verified official primary source for apt_threat_intelligence; routed to Advanced Persistent Threats; ICS/OT Threat Intelligence; Supply Chain and Critical Infrastructure. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: apt_threat_intelligence. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version,

or claim-scope boundary for apt_threat_intelligence materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of apt_threat_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that apt_threat_intelligence claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_cisa_aa24_038a_volt_typhoon retained.

NSA & CISA. Control system defense: Know the opponent, 2022. URL https://media.defense.gov/2022/Sep/22/2003083007/-1/-1/0/CSA_ICS_Know_the_Opponent_.PDF. Verified official primary source for ics_ot_security_standards; routed to ICS/OT Security; Advanced Persistent Threats; MITRE ATT&CK for ICS. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: ics_ot_security_standards. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for ics_ot_security_standards materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of ics_ot_security_standards and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that ics_ot_security_standards claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_cisa_nsa_ics_know_opponent_2022 retained.

Robert M. Clark. Geospatial intelligence: Origins and evolution (georgetown up, 2020), 2020. URL https://press.georgetown.edu/Book/Geospatial-Intelligence. Verified scholarly book metadata source for geoint_tradecraft; routed to GEOINT history and doctrine; remote sensing intelligence; IMINT tradecraft. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: geoint_tradecraft. Source tier: scholarly_book_metadata. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for geoint_tradecraft materially changes. Verification method: direct_publisher_or_catalog_record_review. Claim scope: Supports bounded AGEINT discussion of geoint_tradecraft and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that geoint_tradecraft claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_clark_2020_geospatial_intelligence retained; stale or indirect proposal URL replaced with direct source record.

European Commission. Ai act, 2026a. URL https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai. Official European Commission AI Act implementation page for risk tiers, prohibited practices, GPAI obligations, governance bodies, and phased application. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: ai_conformity_compliance. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: AI Act implementation date, delegated act, guidance, or harmonised-standard status changes. Verification method: direct_official_page_review. Claim scope: AI Act compliance mapping, risk classification, governance timing, and enforcement context. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

European Commission. European ai office, 2026b. URL https://digital-strategy.ec.europa.eu/en/policies/ai-office. Official European Commission source for AI Office responsibilities, GPAI oversight, enforcement coordination, codes of practice, and AI Act implementation. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: ai_conformity_compliance. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: AI Office enforcement role, GPAI implementation, code status, or page ownership changes. Verification method: direct_official_page_review. Claim scope: AI conformity governance, public oversight, GPAI supervision, and institutional accountability. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

European Commission. Common european data spaces, 2026c. URL https://digital-strategy.ec.europa.eu/en/policies/data-spaces. Official European Commission source for Common European Data Spaces, single-market data governance, cross-domain infrastructures, and interoperability specifications. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: cross_border_data_spaces. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: data-space rollout, domain list, reference architecture, or interoperability update. Verification method: direct_official_page_review. Claim scope: cross-border data-sharing infrastructure, domain data spaces, and trustworthy access rules. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

European Commission. Data act explained, 2026d. URL https://digital-strategy.ec.europa.eu/en/policies/data-act-explained. Official European Commission source explaining Data Act access, use, connected-product data, interoperability, and cross-sector data availability. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: cross_border_data_spaces. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: Data Act implementation, FAQs, interoperability guidance, or Commission simplification changes. Verification method: direct_official_page_review. Claim scope: industrial data access, interoperability, user rights, and cross-sector data availability. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

European Commission. European data governance act, 2026e. URL https://digital-strategy.ec.europa.eu/en/policies/data-governance-act. Official European Commission source for data-sharing trust, data intermediaries, public-sector data reuse, data altruism, and European Data Spaces. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: cross_border_data_spaces. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: Data Governance Act application, EDIB guidance, data intermediary, or data altruism update. Verification method: direct_official_page_review. Claim scope: trusted data sharing, cross-sector reuse, data intermediaries, and data-space governance. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

European Commission. A european strategy for data, 2026f. URL https://digital-strategy.ec.europa.eu/en/policies/strategy-data. Official European Commission strategy source for single-market data, data sovereignty, common data spaces, and rights-preserving innovation. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: cross_border_data_spaces. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: European data strategy update, policy package change, or data-space program update. Verification method: direct_official_page_review. Claim scope: data sovereignty, data economy strategy, rights-preserving reuse, and cross-border governance. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

European Commission. Digital education action plan 2021-2027, 2026g. URL https://education.ec.europa.eu/focus-topics/digital-education/action-plan. Official European Commission source for digital education policy, digital skills, AI in education, teacher capacity, and assessment readiness. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: education_assessment. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: Commission action-plan update, digital skills initiative, or education AI guidance changes. Verification method: direct_official_page_review. Claim scope: education governance, digital competence, instructor preparation, and AI readiness. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

European Commission. General-purpose ai code of practice, 2026h. URL https://digital-strategy.ec.europa.eu/en/policies/ai-code-practice. Official European Commission source for GPAI Code of Practice drafting, transparency, copyright, safety, security, and AI Act implementation support. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: ai_conformity_compliance. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: GPAI code text, signatory status, Commission assessment, or AI Act timeline changes. Verification method:

direct_official_page_review. Claim scope: GPAI compliance scaffolding, documentation expectations, safety duties, and copyright transparency. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

OASIS Cyber Threat Intelligence Technical Committee. Taxii version 2.1, 2021. URL https://docs.oasis-open.org/cti/taxii/v2.1/taxii-v2.1.html. OASIS CTI transport standard for defensive threat-intelligence exchange channels, collections, discovery, and API contracts. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: cyber_threat_intelligence. Source tier: international_standard. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

OASIS Cyber Threat Intelligence Technical Committee. Stix version 2.1, 2025. URL https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html. OASIS CTI standard for expressing cyber threat and observable information with structured objects, relationships, sightings, and markings. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: cyber_threat_intelligence. Source tier: international_standard. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

United States Intelligence Community. Artificial intelligence ethics framework for the intelligence community, 2020a. URL https://www.intelligence.gov/ai/ai-ethics-framework. Official IC framework for AI goals, authorities, human judgment, bias mitigation, testing, documentation, explainability, and review. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: ai_ethics_data_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

United States Intelligence Community. Principles of artificial intelligence ethics for the intelligence community, 2020b. URL https://www.intelligence.gov/ai/principles-of-ai-ethics. Official IC principles for lawful, accountable, objective, human-centered, secure, resilient, and science-informed AI. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: ai_ethics_data_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

United States Intelligence Community. How the ic works, 2026. URL https://www.intelligence.gov/how-the-ic-works. Official public explanation of the intelligence cycle, collection disciplines, dissemination, evaluation, oversight, and partners. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: governed_intelligence_cycle. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

United States Congress. Intelligence reform and terrorism prevention act of 2004, 2004. URL https://www.govinfo.gov/link/plaw/108/public/458. Official GovInfo public law record establishing post-9/11 intelligence reform requirements including alternative analysis and analytic integrity provisions. Checked as of 2026-06-11. Citation role: curriculum_anchor. Source lane: intelligence_failure_postmortem. Source tier: official_law. Refresh cadence: biennial. Refresh trigger: Refresh if GovInfo metadata or statutory-citation links change. Verification method: official_law_record_review. Claim scope: Supports claims that post-9/11 reforms created statutory pressure for analytic integrity and alternative analysis. Stakeholder role: curriculum designer; governance reviewer; public-sector analyst. Assurance use: Links tradecraft standards to public-law reform context without turning law into technique guidance. Rights dimension: public-domain legal source; preserve statutory context. GovInfo public law landing page verified live 2026-06-11; use for statutory reform context, not implementation-detail claims.

U.S. Congress. Fisa 1978 - govinfo (statutes at large), 1978. URL https://www.govinfo.gov/content/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf. Verified official primary source for legal_authorities_surveillance; routed to Legal Authorities and Constraints; oversight of domestic electronic surveillance. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: legal_authorities_surveillance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for legal_authorities_surveillance materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of legal_authorities_surveillance and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that legal_authorities_surveillance claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_fisa_1978_statute retained.

U.S. Congress. Usa patriot act - govinfo compilation, 2001. URL https://www.govinfo.gov/content/pkg/COMPS-1507/pdf/COMPS-1507.pdf. Verified official primary source for legal_authorities_surveillance; routed to Legal Authorities and Constraints; post-9/11 surveillance expansion. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: legal_authorities_surveillance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for legal_authorities_surveillance materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of legal_authorities_surveillance and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that legal_authorities_surveillance claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_usa_patriot_act_2001 retained.

U.S. Congress. Usa freedom act - govinfo, 2015. URL https://www.govinfo.gov/content/pkg/PLAW-114publ23/pdf/PLAW-114publ23.pdf. Verified official primary source for legal_authorities_surveillance; routed to Legal Authorities and Constraints; surveillance reform and civil liberties. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: legal_authorities_surveillance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for legal_authorities_surveillance materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of legal_authorities_surveillance and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that legal_authorities_surveillance claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_usa_freedom_act_2015 retained.

World Wide Web Consortium. Prov-o: The prov ontology, 2013a. URL https://www.w3.org/TR/prov-o/. W3C Recommendation for the PROV ontology supporting machine-readable provenance relationships among entities, activities, agents, and roles. Checked as of 2026-05-22. Citation role:

curriculum_anchor. Source lane: model_data_provenance. Source tier: international_standard. Refresh cadence: annual. Refresh trigger: W3C Recommendation errata, ontology update, or provenance best-practice change. Verification method: direct_standards_page_review. Claim scope: machine-readable source lineage, claim ledgers, transformation records, and agent roles. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

World Wide Web Consortium. Prov overview, 2013b. URL https://www.w3.org/TR/prov-overview/. W3C Recommendation overview for provenance interchange, entities, activities, agents, and provenance-family specifications. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: model_data_provenance. Source tier: international_standard. Refresh cadence: annual. Refresh trigger: W3C PROV errata, successor work, or provenance vocabulary update. Verification method: direct_standards_page_review. Claim scope: provenance modeling, source lineage, transformation evidence, and claim-ledger vocabulary. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

World Wide Web Consortium. Data on the web best practices, 2017. URL https://www.w3.org/TR/dwbp/. W3C Recommendation for publishing data with metadata, licenses, provenance, quality, versioning, identifiers, and machine-readable formats. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: model_data_provenance. Source tier: international_standard. Refresh cadence: annual. Refresh trigger: W3C best-practice update, errata, or linked data publication guidance change. Verification method: direct_standards_page_review. Claim scope: dataset publication, provenance, quality, machine readability, identifiers, and reuse conditions. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

World Wide Web Consortium. Decentralized identifiers (dids) v1.0, 2022. URL https://www.w3.org/TR/did-core/. W3C Recommendation for decentralized identifiers, DID documents, verification methods, service endpoints, privacy, and security considerations. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: agent_interoperability_standards. Source tier: international_standard. Refresh cadence: annual. Refresh trigger: W3C Recommendation, errata, DID method guidance, or registry changes. Verification method: direct_standards_page_review. Claim scope: identifier design, verification methods, agent identity analogies, and provenance controls. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

World Wide Web Consortium. Web of things (wot) architecture 1.1, 2023a. URL https://www.w3.org/TR/wot-architecture11/. W3C Recommendation for Web of Things architecture, thing models, security considerations, interoperability, and application patterns. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: agent_interoperability_standards. Source tier: international_standard. Refresh cadence: annual. Refresh trigger: W3C Recommendation, errata, successor specification, or WoT architecture update. Verification method: direct_standards_page_review. Claim scope: tool and thing interoperability, cyber-physical interface modeling, and security-aware architecture. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

World Wide Web Consortium. Web of things (wot) discovery, 2023b. URL https://www.w3.org/TR/wot-discovery/. W3C Recommendation for discovering Web of Things resources using directories, metadata, privacy, and security considerations. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: agent_interoperability_standards. Source tier: international_standard. Refresh cadence: annual. Refresh trigger: W3C Recommendation, errata, successor specification, or discovery security update. Verification method: direct_standards_page_review. Claim scope: safe discovery patterns, directory governance, privacy-aware metadata, and interoperability review. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

World Wide Web Consortium. Web of things (wot) thing description 1.1, 2023c. URL https://www.w3.org/TR/wot-thing-description11/. W3C Recommendation for machine-readable thing descriptions, interaction affordances, metadata, security, and protocol bindings. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: agent_interoperability_standards. Source tier: international_standard. Refresh cadence: annual. Refresh trigger: W3C Recommendation, errata, successor specification, or thing-description vocabulary update. Verification method: direct_standards_page_review. Claim scope: machine-readable tool affordances, interface descriptions, security metadata, and binding discipline. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

World Wide Web Consortium. Data catalog vocabulary (dcat) version 3, 2024. URL https://www.w3.org/TR/vocab-dcat-3/. W3C Recommendation for cataloging datasets and data services with metadata, distributions, provenance, access, and quality signals. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: model_data_provenance. Source tier: international_standard. Refresh cadence: annual. Refresh trigger: W3C Recommendation, vocabulary term, errata, or data-catalog practice update. Verification method: direct_standards_page_review. Claim scope: dataset cataloging, metadata records, provenance fields, and data-service documentation. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

World Wide Web Consortium. Verifiable credential data integrity 1.0, 2025a. URL https://www.w3.org/TR/vc-data-integrity/. W3C Recommendation for data integrity proofs, proof sets, proof chains, verification methods, and transformed data protection in verifiable credentials. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: model_data_provenance. Source tier: technical_standard. Refresh cadence: semiannual. Refresh trigger: W3C VC Data Integrity recommendation, errata, cryptosuite, or implementation report changes. Verification method: direct_standards_page_review. Claim scope: data integrity proofs, credential provenance, verification records, and signed evidence chains. Stakeholder role: data steward, verifier, instructor, learner, and provenance auditor. Assurance use: data lineage registry and verifiable-evidence check. Rights dimension: data integrity, provenance, authenticity, and accountable reuse. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

World Wide Web Consortium. Verifiable credentials data model v2.0, 2025b. URL https://www.w3.org/TR/vc-data-model-2.0/. W3C Recommendation for verifiable credentials, issuers, holders, verifiers, security, privacy, internationalization, and accessibility considerations. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: agent_interoperability_standards. Source tier: international_standard. Refresh cadence: annual. Refresh trigger: W3C Recommendation, errata, implementation report, or data-model update. Verification method: direct_standards_page_review. Claim scope: credential provenance, trust model, machine-verifiable claims, and identity evidence. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Jeffrey R. Cooper. Curing analytic pathologies: Pathways to improved intelligence analysis, 2005. URL https://www.cia.gov/resources/csi/books-monographs/curing-analytic-pathologies/. CIA Center for the Study of Intelligence monograph on analytic pathologies, self-correction, and intelligence-process reform. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: analytic_tradecraft_evidence. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: CIA CSI page, monograph URL, or public release status changes. Verification method: direct_official_page_review. Claim scope: Supports bounded claims about analytic-culture reform, self-correction, peer challenge, and limits of linear intelligence-cycle metaphors. Stakeholder role: analytic tradecraft instructor; curriculum designer; reviewer. Assurance use: Adds institutional self-critique to SAT evidence boundaries and analytic process reform lessons. Rights dimension: public CIA CSI monograph used for education and source-backed critique. Direct CIA CSI book page verified live 2026-06-15; used for analytic-culture reform context, not as proof that any specific SAT improves accuracy.

North American Electric Reliability Corporation. Nerc cip reliability standards (cip-002 through cip-015), NERC. URL https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx. Verified official primary source for ics_ot_security_standards; routed to ICS/OT Security; Critical Infrastructure Protection; Threat Intelligence Sharing for Critical Infrastructure. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: ics_ot_security_standards.

Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for ics_ot_security_standards materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of ics_ot_security_standards and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that ics_ot_security_standards claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_nerc_cip_standards retained.

Michael Landon-Murray; Wahid Saifuddin; Stephen Coulthart. Structured analytic techniques in an intelligence fusion centre: A survey of analyst perspectives and use, 2025. URL https://doi.org/10.1080/18335330.2024.2436384. Peer-reviewed survey of SAT perspectives and use in an intelligence fusion-centre context, useful for adoption and training caveats. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: sat_evaluation_evidence. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: Publisher metadata, DOI record, correction, or retraction status changes. Verification method: crossref_doi_metadata_review. Claim scope: Supports bounded claims about SAT use and perceptions in fusion-centre practice, not direct proof of analytic accuracy gains. Stakeholder role: curriculum designer; analytic standards trainer; evaluation lead. Assurance use: Adds current practice evidence while keeping adoption, perception, and efficacy as separate claims. Rights dimension: copyrighted scholarly article; cite DOI metadata and summarize sparingly. Crossref DOI metadata verified live 2026-06-15 for title, authors, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.

Stephen Coulthart. Why do analysts use structured analytic techniques? an in-depth study of an american intelligence agency, 2016. URL https://doi.org/10.1080/02684527.2016.1140327. Peer-reviewed study of why analysts use SATs, supporting adoption, training, and organizational-context claims rather than universal efficacy claims. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: sat_evaluation_evidence. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: Publisher metadata, DOI record, correction, or retraction status changes. Verification method: crossref_doi_metadata_review. Claim scope: Supports bounded claims about SAT adoption motives and organizational use, not empirical proof that SATs improve accuracy across tasks. Stakeholder role: curriculum designer; analytic standards trainer; evaluation lead. Assurance use: Separates usage and institutionalization evidence from efficacy evidence in SAT lessons. Rights dimension: copyrighted scholarly article; cite DOI metadata and summarize sparingly. Crossref DOI metadata verified live 2026-06-15 for title, author, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.

Stephen J. Coulthart. An evidence-based evaluation of 12 core structured analytic techniques, 2017. URL https://doi.org/10.1080/08850607.2016.1230706. Peer-reviewed evaluation of core SATs used to qualify claims about where specific techniques may or may not have evidence support. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: sat_evaluation_evidence. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: Publisher metadata, DOI record, correction, or retraction status changes. Verification method: crossref_doi_metadata_review. Claim scope: Supports bounded technique-specific evidence-boundary claims about SATs and discourages treating the category as uniformly validated. Stakeholder role: curriculum designer; analytic standards trainer; evaluation lead. Assurance use: Forces SAT exercises to distinguish doctrine, classroom utility, and empirical support by technique. Rights dimension: copyrighted scholarly article; cite DOI metadata and summarize sparingly. Crossref DOI metadata verified live 2026-06-15 for title, author, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.

National Research Council. Intelligence analysis for tomorrow: Advances from the behavioral and social sciences, 2011. URL https://nap.nationalacademies.org/catalog/13040/intelligence-analysis-for-tomorrow-advances-from-the-behavioral-and-social-sciences. National Academies report connecting behavioral and social science to intelligence-analysis training, judgment, and organizational improvement. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: analytic_cognition_and_bias. Source tier: scholarly_public_report. Refresh cadence: annual. Refresh trigger: National Academies record, DOI metadata, edition, or access status changes. Verification method: publisher_record_and_crossref_doi_review. Claim scope: Supports bounded claims about using behavioral and social science to improve analysis, training, and evaluation without claiming technique-level guarantees. Stakeholder role: curriculum designer; cognition reviewer; evaluation lead. Assurance use: Links analytic-cognition lessons to a public expert-report baseline and keeps SAT claims evidence-sensitive. Rights dimension: National Academies publication metadata and public report access; cite and summarize sparingly. National Academies publisher record verified live 2026-06-15; Crossref DOI metadata for 10.17226/13040 verified title, publisher, and year.

National Counterintelligence and Security Center. The national counterintelligence strategy, 2024. URL https://www.odni.gov/index.php/ncsc-features/2741-the-national-counterintelligence-strategy-of-the-united-states-of-america. Official strategy for defensive CI integration, foreign-intelligence threat awareness, strategic advantage protection, and future readiness. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: counterintelligence_source_integrity. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Counterintelligence and Security Center. National counterintelligence strategy 2020-2022 (ncsc/odni), NCSCa. URL https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf. Verified official primary source for counterintelligence_strategy; routed to Counterintelligence (fundamentals + against non-state actors). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: counterintelligence_strategy. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for counterintelligence_strategy materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of counterintelligence_strategy and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that counterintelligence_strategy claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_ncsc_national_ci_strategy_2020 retained.

National Counterintelligence and Security Center. National counterintelligence strategy 2024 (ncsc/odni), NCSCb. URL https://www.dni.gov/files/NCSC/documents/features/NCSC_CI_Strategy-pages-20240730.pdf. Verified official primary source for counterintelligence_strategy; routed to Counterintelligence (fundamentals + against non-state actors). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: counterintelligence_strategy. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for counterintelligence_strategy materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of counterintelligence_strategy and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that counterintelligence_strategy claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_ncsc_national_ci_strategy_2024 retained.

Inc. CrewAI. Crewai documentation, 2025. URL https://docs.crewai.com. Verified professional documentation source for agentic_framework_docs; routed to CrewAI Multi-Agent appendix; Frameworks & Infrastructure. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: agentic_framework_docs. Source tier:

professional_documentation. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for agentic_framework_docs materially changes. Verification method: direct_professional_documentation_review. Claim scope: Supports bounded AGEINT discussion of agentic_framework_docs and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that agentic_framework_docs claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key professional_crewai_documentation retained.

Cybersecurity and Infrastructure Security Agency. Ai red teaming: Applying software tevv for ai evaluations, 2024a. URL https://www.cisa.gov/news-events/news/ai-red-teaming-applying-software-tevv-ai-evaluations. CISA guidance connecting AI red teaming to testing, evaluation, verification, and validation for security and safety assurance. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: ai_red_team_assurance. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: CISA AI red-teaming, TEVV, security-evaluation, or AI-testing guidance changes. Verification method: direct_official_page_review. Claim scope: AI red-team assurance, TEVV framing, software safety evaluation, and critical-infrastructure security testing. Stakeholder role: red-team reviewer, evaluator, critical-infrastructure steward, instructor, and learner. Assurance use: AI red-team TEVV crosswalk and assurance critique. Rights dimension: safety, security, fit-for-purpose evaluation, reliability, and accountable testing. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Cybersecurity and Infrastructure Security Agency. Preparing for and mitigating foreign influence operations, 2024b. URL https://www.cisa.gov/resources-tools/resources/cisa-insights-preparing-and-mitigating-foreign-influence-operations-targeting-critical. Official CISA guidance on foreign influence operations targeting critical infrastructure. Checked as of 2026-05-21. Citation role: source_quality_anchor. Source lane: source_quality_spine. Source tier: source_quality_anchor. Refresh cadence: semiannual. Refresh trigger: source version, legal status, standard revision, or official guidance changes. Verification method: direct_source_url_review. Claim scope: baseline source-quality guardrail for generated AGEINT curriculum claims. Stakeholder role: curriculum maintainer, instructor, reviewer, and learner. Assurance use: source-quality triangulation and claim-boundary review. Rights dimension: source transparency, accountability, and evidence traceability. Directly verified official CISA source URL.

Cybersecurity and Infrastructure Security Agency. Creating and maintaining a definitive view of your operational technology (ot) architecture, 2025a. URL https://www.cisa.gov/resources-tools/resources/creating-and-maintaining-definitive-view-your-operational-technology-ot-architecture. CISA guidance on creating and maintaining a definitive view of OT architecture, used as an assurance-evidence anchor for cyber-physical readiness. Checked as of 2026-05-24. Citation role: curriculum_anchor. Source lane: assurance_evaluation_evidence. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: CISA OT architecture guidance, architecture record, communication map, definitive-view process, or change-control recommendation update. Verification method: direct_official_page_review. Claim scope: definitive OT architecture, asset and communication records, evidence baseline, cyber-physical assurance, and change-control review. Stakeholder role: OT architect, assurance reviewer, operator, instructor, and learner. Assurance use: definitive OT architecture record, evidence map, review cadence, change-control packet, and tabletop assurance baseline. Rights dimension: safety, availability, operational resilience, accountable architecture evidence, auditability, and defensive readiness. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Cybersecurity and Infrastructure Security Agency. Secure by demand: Priority considerations for operational technology owners and operators when selecting digital products, 2025b. URL https://www.cisa.gov/resources-tools/resources/secure-demand-priority-considerations-operational-technology-owners-and-operators-when-selecting. CISA Secure by Demand considerations for OT owners and operators selecting digital products, used for vendor-governance and procurement review. Checked as of 2026-05-24. Citation role: curriculum_anchor. Source lane: procurement_vendor_governance. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: CISA Secure by Demand, OT procurement, vendor security, priority consideration, or owner/operator guidance changes. Verification method: direct_official_page_review. Claim scope: OT procurement, secure-by-demand selection criteria, vendor accountability, operational resilience, and cyber-physical due diligence. Stakeholder role: OT owner, procurement official, vendor assessor, instructor, and learner. Assurance use: OT procurement checklist, vendor security criteria, defensible selection evidence, and lifecycle assurance review. Rights dimension: safety, resilience, accountable procurement, vendor transparency, service continuity, and due care. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Cybersecurity and Infrastructure Security Agency. Cross-sector cybersecurity performance goals, 2026a. URL https://www.cisa.gov/cybersecurity-performance-goals. Official prioritized baseline of IT and OT cybersecurity practices for critical-infrastructure risk reduction and maturity assessment. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: ics_ot_defense. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Cybersecurity and Infrastructure Security Agency. Election security, 2026b. URL https://www.cisa.gov/topics/election-security. Official CISA election-security source for public-resilience, foreign-influence awareness, rumor control, and defensive communication framing. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: cognitive_influence_security. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Cybersecurity and Infrastructure Security Agency. Ics recommended practices, 2026c. URL https://www.cisa.gov/resources-tools/resources/ics-recommended-practices. Official defensive ICS practice library for defense-in-depth, forensics, incident response, and remote access. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: ics_ot_defense. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Cybersecurity and Infrastructure Security Agency. Known exploited vulnerabilities catalog, 2026d. URL https://www.cisa.gov/known-exploited-vulnerabilities-catalog. Official catalog for prioritizing known exploited vulnerabilities as defensive triage inputs, not as exploitation instructions. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: cyber_threat_intelligence. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Cybersecurity and Infrastructure Security Agency. Secure by design, 2026e. URL https://www.cisa.gov/securebydesign. Official secure-by-design program source for customer security outcomes, radical transparency, leadership accountability, and safer defaults. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: agentic_ai_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Cybersecurity and Infrastructure Security Agency. Cisa tabletop exercise packages, 2026f. URL https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages. Official exercise packages for cyber, physical, ICS, ransomware, and convergence tabletop scenarios. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: ics_ot_defense. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Cybersecurity, Infrastructure Security Agency, and international partners. Joint guidance on deploying ai systems securely, 2024. URL https://www.cisa.gov/news-events/alerts/2024/04/15/joint-guidance-deploying-ai-systems-securely. CISA joint guidance for deploying AI systems securely, used as a release/change-control anchor for AI-enabled services. Checked as of 2026-05-24. Citation role: curriculum_anchor. Source lane: secure_release_change_control. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: CISA or partner AI deployment guidance, secure configuration, monitoring, release, or incident-management update. Verification method: direct_official_page_review. Claim scope: secure AI deployment, threat modeling, system integration, secure configuration, monitoring, incident planning, and responsible release. Stakeholder role: AI system owner, security reviewer, release manager, instructor, and learner. Assurance use: secure AI deployment gate, change-control review, rollback evidence, monitoring threshold, and incident trigger. Rights dimension: security, reliability, safety, accountability, privacy, operational resilience, and public trust. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Cybersecurity, Infrastructure Security Agency, and partners. Cisa and partners release asset inventory guidance to strengthen operational technology security, 2025a. URL https://www.cisa.gov/news-events/news/cisa-and-partners-release-asset-inventory-guidance-strengthen-operational-technology-security. CISA and partners' asset-inventory guidance for strengthening operational technology security and keeping OT records reviewable. Checked as of 2026-05-24. Citation role: curriculum_anchor. Source lane: records_retention_auditability. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: CISA OT asset inventory guidance, partner release, asset-record field, inventory process, or OT security visibility update. Verification method: direct_official_page_review. Claim scope: OT asset inventory, authoritative records, operational technology security, owner evidence, and defensive visibility. Stakeholder role: OT asset owner, records reviewer, security engineer, instructor, and learner. Assurance use: OT asset-inventory register, change evidence, owner field review, and auditability packet. Rights dimension: safety, service continuity, operational resilience, accountable records, auditability, and change traceability. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Cybersecurity, Federal Bureau of Investigation Infrastructure Security Agency, National Security Agency, and international partners. Ai data security: Best practices for securing data used to train and operate ai systems, 2025b. URL https://media.defense.gov/2025/May/22/2003720601/-1/-1/0/CSI_AI_DATA_SECURITY.PDF. Joint official cybersecurity information sheet on best practices for securing data used to train and operate AI systems across the lifecycle. Checked as of 2026-06-11. Citation role: curriculum_anchor. Source lane: model_data_provenance. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: CISA, NSA, FBI, or partner AI data-security lifecycle guidance changes. Verification method: direct_official_pdf_review. Claim scope: AI data security for data used to train, test, deploy, and operate AI systems, including provenance, integrity, confidentiality, lifecycle controls, and trustworthy AI outcomes. Stakeholder role: data steward, model owner, procurement reviewer, release reviewer, instructor, and learner. Assurance use: model/data provenance card, AI data-security control review, training-data integrity checks, operational-data lifecycle mapping, and release-readiness evidence. Rights dimension: data integrity, confidentiality, provenance, privacy, trusted infrastructure, accountable reuse, and trustworthy AI outcomes. Direct official CISA/NSA/FBI partner PDF verified live 2026-06-11; executive summary covers AI data security, lifecycle stages, integrity risks, and best practices.

Parr T. Sajid N. Veselic S. Neacsu V. & Friston K. Da Costa, L. Active inference on discrete state-spaces, 2020. URL https://doi.org/10.1016/j.jmp.2020.102447. A mathematical synthesis of active inference over discrete (POMDP) state-spaces, consolidating the partially observable Markov decision process model used to specify perception, planning, and action selection in agentic systems. Checked as of 2026-06-08. Citation role: curriculum_anchor. Source lane: cognitive_active_inference. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: source URL, DOI, edition/standard version, or claim scope materially changes. Verification method: direct_source_url_review. Claim scope: Discrete-state / POMDP modeling underpinning agentic systems in AGEINT. Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.

DataCite. Datacite metadata schema, 2026. URL https://schema.datacite.org/. Official DataCite schema source for dataset citation metadata, persistent identifiers, creators, dates, relationships, and versioning. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: model_data_provenance. Source tier: research_standard. Refresh cadence: annual. Refresh trigger: schema version, DOI metadata property, controlled vocabulary, or relation-type update. Verification method: direct_standards_page_review. Claim scope: dataset citation, persistent identifiers, source metadata, relation tracking, and version history. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Google DeepMind and Google Research. Architecting trust in artificial epistemic agents, 2026. URL https://arxiv.org/html/2603.02960v1. Google DeepMind arXiv paper defining the epistemic AI agent and proposing demonstrable competence, falsifiability, virtuous behavior, provenance chains, verifier agents, and knowledge sanctuaries. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: model_data_provenance. Source tier: frontier_lab_research. Refresh cadence: annual. Refresh trigger: New arXiv version of the epistemic-agent trust paper, revised trust desiderata, provenance architecture, or successor DeepMind publication changes. Verification method: direct_research_page_review. Claim scope: epistemic AI agents, trust desiderata (competence, falsifiability, virtue), provenance and verifier-agent architecture, and human cognitive risks. Direct source URL verified live (HTTP 200, on-topic DeepMind epistemic-agent arXiv paper) for AGEINT curriculum use.

Harry Deng and UNIDIR. Exploring synthetic data for artificial intelligence and autonomous systems, 2023. URL https://unidir.org/publication/exploring-synthetic-data-for-artificial-intelligence-and-autonomous-systems-a-primer/. UNIDIR primer on synthetic data for artificial intelligence and autonomous systems, used for source-quality and risk caveats around synthetic fixtures and military AI governance. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: model_data_provenance. Source tier: public_domain_primary. Refresh cadence: annual. Refresh trigger: UNIDIR report URL, PDF, synthetic-data governance literature, or autonomous-systems policy materially changes. Verification method: primary_browser_report_page_review. Claim scope: Supports bounded discussion of synthetic data for AI and autonomous systems in international security, including benefits and limitations; not evidence for operational deployment readiness. Stakeholder role: AI governance reviewer, data steward, instructor, policy analyst. Assurance use: synthetic-data risk review, AI-DSS dataset-provenance caveats, and autonomous-systems governance framing. Rights dimension: lawful use, safety, data integrity, bias, human oversight, and international-security responsibility. Direct UNIDIR report page and PDF were verified on 2026-06-15 after the attachment URL had moved; title, author, citation, and scope were visible.

Markus Denzler. Revisiting the psychology of structured analytical techniques, 2024. URL https://doi.org/10.1080/08850607.2023.2243803. Peer-reviewed article revisiting psychological assumptions behind SATs and their relationship to analytic cognition. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: analytic_cognition_and_bias. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: Publisher metadata, DOI record, correction, or retraction status changes. Verification method: crossref_doi_metadata_review. Claim scope: Supports bounded claims about SAT psychology and cognitive assumptions without treating technique use as validated bias elimination. Stakeholder role: cognition reviewer; analytic standards trainer; curriculum designer. Assurance use: Keeps cognitive-security and tradecraft prose explicit about mechanism uncertainty and evidence limits. Rights dimension: copyrighted scholarly article; cite DOI metadata and summarize

sparingly. Crossref DOI metadata verified live 2026-06-15 for title, author, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.

Deppe and Schaal. A conceptual framework and method for a nato act concept for cognitive warfare, 2024. URL https://pmc.ncbi.nlm.nih.gov/articles/PMC11565700/. Open-access PMC article on a NATO ACT cognitive-warfare concept, routed for conceptual and governance framing with explicit evidence-bounded limits. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: cognitive_influence_security. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: PMC record, NATO cognitive-warfare concept literature, or terminology materially changes. Verification method: direct_pmc_page_review. Claim scope: Supports bounded discussion of NATO cognitive-warfare concept development and terminology; not operational doctrine and not evidence for intervention efficacy. Stakeholder role: cognitive-security reviewer, policy instructor, assurance reviewer. Assurance use: NATO cognitive-warfare concept caveat, influence-risk framing, and evidence-bounded classroom boundary. Rights dimension: mental autonomy, democratic accountability, public trust, and non-manipulative education. Direct PMC source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

David R. Mandel; Christopher W. Karvetski; Mandeep K. Dhami. Boosting intelligence analysts' judgment accuracy: What works, what fails?, 2018. URL https://www.cambridge.org/core/journals/judgment-and-decision-making/article/boosting-intelligence-analysts-judgment-accuracy-what-works-what-fails/1530E9DAE8F42B2E8FC2B5FE374DB50F. Open Judgment and Decision Making article comparing ACH, coherentization, and aggregation for intelligence analysts' probability judgments. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: forecasting_calibration_evidence. Source tier: scholarly_peer_reviewed_open. Refresh cadence: annual. Refresh trigger: Publisher metadata, correction, or retraction status changes. Verification method: publisher_open_article_review. Claim scope: Supports bounded claims that calibration, coherentization, and aggregation can complement SATs without making ACH a universal accuracy intervention. Stakeholder role: forecasting instructor; curriculum designer; evaluation lead. Assurance use: Routes SAT automation claims toward accountable judgment support, not analyst replacement. Rights dimension: open scholarly article; cite source and avoid extended quotation. Cambridge Core article page verified live 2026-06-15 for title, authors, journal record, and accessible article metadata.

NSA & FBI. DOE, CISA. Apt cyber tools targeting ics/scada devices (aa22-103a), 2022. URL https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-103a. Verified official primary source for apt_threat_intelligence; routed to Advanced Persistent Threats; ICS/OT Security; MITRE ATT&CK for ICS. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: apt_threat_intelligence. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for apt_threat_intelligence materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of apt_threat_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that apt_threat_intelligence claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_cisa_aa22_103a_apt_ics_scada retained.

Huw Dylan and Nicholas Stivang. Emerging technologies and national security intelligence, 2025. URL https://www.tandfonline.com/doi/full/10.1080/02684527.2025.2565948. Peer-reviewed Intelligence and National Security article on emerging technologies and national security intelligence, used to frame AI and data-system effects as medium-term intelligence-work pressures requiring analytic governance. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: ai_enabled_analysis_boundary. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: journal article, DOI landing page, or scholarly consensus about emerging-technology effects on intelligence work materially changes. Verification method: script_http_200_scholarly_page_review. Claim scope: Supports bounded discussion of how AI, quantum technologies, and data-generating systems may reshape intelligence work; does not prove deployed AGEINT capability or abrupt transformation. Stakeholder role: analyst, AI governance reviewer, instructor, curriculum maintainer. Assurance use: emerging-technology source review, AI-assisted analysis boundary setting, and medium-term tradecraft refresh planning. Rights dimension: accountability, public trust, privacy, and reviewable use of emerging technology in intelligence education. Direct Taylor and Francis source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Krampe R. T. & Tesch-Romer C. Ericsson, K. A. The role of deliberate practice in the acquisition of expert performance, 1993. URL https://eric.ed.gov/?id=EJ471947. Verified scholarly repository record source for cognitive_performance; routed to Productivity Intelligence & Cognitive Performance (cognitive athlete, deliberate practice); Instructor Capstone/Rubric/Red-Team Pack appendix. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: cognitive_performance. Source tier: scholarly_repository_record. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for cognitive_performance materially changes. Verification method: direct_source_url_review. Claim scope: Supports bounded AGEINT discussion of cognitive_performance and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that cognitive_performance claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_ericsson_1993_deliberate_practice retained.

Cardenuto et al. The age of synthetic realities: Challenges and opportunities, 2023a. URL https://arxiv.org/abs/2306.11503. arXiv survey-style source on synthetic realities and AI-generated media risk, used for provenance, detection-limit, and public-trust framing in cognitive-security lessons. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: synthetic_media_provenance. Source tier: scholarly_preprint. Refresh cadence: semiannual. Refresh trigger: arXiv version, synthetic-media detection literature, provenance standards, or misuse patterns materially changes. Verification method: direct_arxiv_page_review. Claim scope: Supports bounded discussion of synthetic realities, generated media, and provenance risk; does not support identity-attack recipes or unrestricted deepfake detection claims. Stakeholder role: cognitive-security reviewer, media-literacy instructor, AI governance reviewer. Assurance use: synthetic media provenance review, deepfake risk caveats, and synthetic-reality classroom examples. Rights dimension: identity protection, consent, provenance, public trust, and harms from synthetic media. Direct arXiv source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Friedman et al. Active inference in modeling conflict, 2021a. URL https://doi.org/10.5281/zenodo.5750935. Zenodo-hosted scholarly source on active inference in modeling conflict, used only for bounded theory-to-scenario analogies and caveated simulation discussion. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: cognitive_active_inference. Source tier: scholarly_preprint. Refresh cadence: annual. Refresh trigger: Zenodo record, DOI metadata, active-inference conflict-modeling literature, or simulation caveats materially changes. Verification method: doi_redirect_primary_record_review. Claim scope: Supports bounded discussion of active-inference modeling in conflict scenarios; AGEINT treats it as theory/simulation context, not operational prediction or targeting evidence. Stakeholder role: theory reviewer, instructor, simulation-method reviewer. Assurance use: active-inference conflict-modeling boundary, simulation caveat, and theory-to-scenario review. Rights dimension: non-escalatory education, scientific transparency, human accountability, and avoidance of live targeting. DOI redirected to the Zenodo primary record with HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Gaeta et al. Situation awareness in intelligence scenarios, 2021b. URL https://pmc.ncbi.nlm.nih.gov/articles/PMC8325623/. Open-access PMC article on situation awareness in intelligence scenarios, useful for analytic-cognition lessons and scenario-review vocabulary. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: analytic_cognition_and_bias. Source tier: scholarly_peer_reviewed. Refresh cadence:

annual. Refresh trigger: PMC record, situation-awareness literature, intelligence-training evidence, or claim scope materially changes. Verification method: direct_pmc_page_review. Claim scope: Supports bounded discussion of situation awareness in intelligence scenarios; does not prove AGEINT learning outcomes or operational analyst performance. Stakeholder role: analyst, instructor, cognitive-workload reviewer. Assurance use: situation-awareness scenario review, analyst-cognition caveats, and intelligence-training source support. Rights dimension: analyst comprehension, transparency, cognitive workload, and accountable training. Direct PMC source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Golob et al. Human cognition through the lens of social engineering cyberattacks, 2020. URL https://pmc.ncbi.nlm.nih.gov/articles/PMC7554349/. Open-access PMC article on human cognition in social-engineering cyberattacks, routed as defensive awareness and cognitive-security evidence with operational details excluded. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: cognitive_influence_security. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: PMC record, social-engineering cognition literature, or cyber-awareness evidence materially changes. Verification method: direct_pmc_page_review. Claim scope: Supports defensive cognitive framing of social-engineering cyberattacks; excludes persuasion scripts, pretexting recipes, credential harvesting, and live targeting. Stakeholder role: security-awareness instructor, cognitive-security reviewer, cyber defender. Assurance use: social-engineering cognition review, defensive awareness framing, and no-playbook safety boundary. Rights dimension: privacy, consent, user protection, psychological safety, and defensive education. Direct PMC source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Huang et al. Challenges of artificial intelligence to cognitive security and safety, 2023b. URL https://sands.edpsciences.org/articles/sands/pdf/2023/01/sands20230010.pdf. Open-access Safety and Security article on AI challenges to cognitive security and safety, routed as bounded cognitive-security risk context. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: cognitive_influence_security. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: article URL, cognitive-security AI literature, or safety taxonomy materially changes. Verification method: script_http_200_scholarly_pdf_review. Claim scope: Supports high-level scholarly discussion of AI challenges to cognitive security and safety; does not establish universal cognitive-security efficacy or manipulation countermeasures. Stakeholder role: cognitive-security reviewer, instructor, AI safety reviewer. Assurance use: cognitive-security risk caveat, AI safety source routing, and resilience-evidence calibration. Rights dimension: mental autonomy, safety, public trust, transparency, and non-manipulative resilience education. Direct journal PDF URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Karl Friston et al. Active inference and epistemic value, 2015. URL https://pubmed.ncbi.nlm.nih.gov/25689102/. PubMed-indexed active-inference source on epistemic value, routed as theory support for bounded analogies in the cognitive-active-inference profile. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: cognitive_active_inference. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: PubMed record, DOI metadata, active-inference theory literature, or claim-scope interpretation materially changes. Verification method: direct_pubmed_page_review. Claim scope: Supports formal active-inference theory discussion around epistemic value and policy selection; does not validate AGEINT product performance or autonomous intent detection. Stakeholder role: theory reviewer, instructor, method designer. Assurance use: active-inference theory boundary, epistemic-value caveat, and formal-source review. Rights dimension: epistemic humility, transparent analogy, scientific caveat, and human accountability. Direct PubMed source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Karl Friston et al. Uncertainty, epistemics and active inference, 2017. URL https://pmc.ncbi.nlm.nih.gov/articles/PMC5721148/. Open-access PMC article on uncertainty, epistemics, and active inference, encoded for theory boundaries and claim-calibration around active-inference analogies. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: cognitive_active_inference. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: PMC record, DOI metadata, active-inference theory literature, or analogy caveats materially changes. Verification method: direct_pmc_page_review. Claim scope: Supports scholarly discussion of uncertainty, epistemics, and active inference; not proof that AGEINT agents possess cognition or operational competence. Stakeholder role: theory reviewer, instructor, governance reviewer. Assurance use: active-inference uncertainty caveat, theory-to-analogy review, and non-overclaiming checks. Rights dimension: scientific transparency, epistemic humility, human accountability, and non-deceptive explanation. Direct PMC source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Khlaaf et al. Mind the gap: Foundation models and the covert proliferation of military intelligence, surveillance, target acquisition, and reconnaissance, 2024a. URL https://arxiv.org/html/2410.14831v1. arXiv HTML source on foundation models and covert proliferation of military ISTAR capabilities, routed as a risk-boundary source for synthetic and defensive education. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: ai_enabled_analysis_boundary. Source tier: scholarly_preprint. Refresh cadence: semiannual. Refresh trigger: arXiv version, military-AI risk literature, or foundation-model capability discussion materially changes. Verification method: direct_arxiv_html_review. Claim scope: Supports bounded discussion of foundation-model risks for military intelligence, surveillance, target acquisition, and reconnaissance; AGEINT uses it for risk framing, not for operational ISTAR guidance. Stakeholder role: AI safety reviewer, intelligence educator, policy analyst, red-team reviewer. Assurance use: foundation-model risk boundary, ISTAR claim calibration, and covert-proliferation scenario review. Rights dimension: non-proliferation, civilian protection, escalation risk, and human accountability. Direct arXiv HTML source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Mandeep K. Dhami et al. Analysis of competing hypotheses in intelligence analysis, 2019. URL https://onlinelibrary.wiley.com/doi/10.1002/acp.3550. Applied Cognitive Psychology article on Analysis of Competing Hypotheses in intelligence analysis, routed as empirical/SAT evidence with explicit limitations. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: sat_evaluation_evidence. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: Wiley article URL, DOI metadata, ACH evidence literature, or SAT evaluation consensus materially changes. Verification method: script_http_200_scholarly_page_review. Claim scope: Supports bounded scholarly discussion of ACH in intelligence analysis; does not imply ACH universally eliminates bias or guarantees analytic accuracy. Stakeholder role: analyst, method instructor, reviewer, red-team facilitator. Assurance use: ACH method evidence review, SAT caveat writing, and analytic-bias classroom comparison. Rights dimension: analytic fairness, uncertainty communication, cognitive-bias awareness, and accountable review. Direct Wiley source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Mandeep K. Dhami et al. Task structure, confirmation bias, and the generation of alternative hypotheses, 2024b. URL https://cognitiveresearchjournal.springeropen.com/articles/10.1186/s41235-024-00560-y. Cognitive Research article on how task structure affects confirmation bias and alternative hypotheses, useful for designing negative controls around ACH and SAT exercises. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: sat_evaluation_evidence. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: SpringerOpen article URL, DOI metadata, task-structure literature, or confirmation-bias evidence materially changes. Verification method: script_http_200_scholarly_page_review. Claim scope: Supports bounded discussion of task structure and confirmation bias in hypothesis generation; not a universal debiasing or intelligence-success claim. Stakeholder role: method instructor, analyst, reviewer, learner. Assurance use: confirmation-bias negative-control design, alternative-hypothesis checklist review, and task-structure caveats. Rights dimension: analytic fairness, cognitive-bias mitigation, transparent alternatives, and reviewer challenge. Direct SpringerOpen source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Miles Brundage et al. The malicious use of artificial intelligence: Forecasting, prevention, and mitigation, 2018. URL https://arxiv.org/abs/1802.07228. Foundational public report on malicious uses of AI, encoded for defensive taxonomy, safe-substitution, and governance framing in synthetic classroom work. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: ai_red_team_assurance. Source tier: scholarly_report. Refresh cadence: annual. Refresh trigger: AI misuse taxonomy, cited source URL, or consensus risk framing materially changes. Verification method:

direct_arxiv_page_review. Claim scope: Supports high-level AI misuse taxonomy and defensive risk analysis only; AGEINT excludes operational instructions, target selection, evasion, and exploit procedures. Stakeholder role: red-team reviewer, AI governance lead, instructor, safety reviewer. Assurance use: AI misuse taxonomy review, red-team scenario boundaries, and safe substitution design. Rights dimension: safety, security, public trust, civil liberties, and defensive risk communication. Direct arXiv source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Ortega et al. The ai incident regime, 2025a. URL https://arxiv.org/html/2503.19887. arXiv HTML source on AI incident regimes, routed as comparative governance context for incident reporting, risk exceptions, and assurance evidence. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: agent_incident_response. Source tier: scholarly_preprint. Refresh cadence: semiannual. Refresh trigger: arXiv version, AI incident reporting regimes, official policy changes, or scholarly governance literature materially changes. Verification method: direct_arxiv_html_review. Claim scope: Supports bounded scholarly discussion of AI incident regimes and reporting design; does not replace official incident-reporting standards already encoded in AGEINT. Stakeholder role: AI incident reviewer, legal/oversight reviewer, instructor, risk owner. Assurance use: AI incident-regime comparison, governance-exception review, and reporting-system caveats. Rights dimension: transparency, accountability, due process, public safety, and affected-party protection. Direct arXiv HTML source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Penmetsa et al. Adversarial machine learning in cybersecurity, 2025b. URL https://ejaset.com/index.php/journal/article/view/294. Journal article reviewing adversarial machine learning in cybersecurity, encoded as supplemental scholarly support for defensive AI red-team assurance. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: ai_red_team_assurance. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: journal article URL, adversarial-ML literature, AI security taxonomy, or defensive testing guidance materially changes. Verification method: script_http_200_scholarly_page_review. Claim scope: Supports defensive literature-review discussion of adversarial machine learning in cybersecurity; excludes exploit, evasion, and bypass procedures. Stakeholder role: AI security reviewer, cyber instructor, red-team reviewer. Assurance use: adversarial-ML literature review, cyber-AI control mapping, and defensive testing caveats. Rights dimension: security, system integrity, safety, accountable testing, and defensive education. Direct journal source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Ryan Smith et al. A step-by-step tutorial on active inference and its application to empirical data, 2022. URL https://pmc.ncbi.nlm.nih.gov/articles/PMC8956124/. Open-access tutorial on active inference and empirical-data applications, routed as a learner-facing formal-method source for bounded AGEINT analogies. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: cognitive_active_inference. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: PMC record, active-inference tutorial literature, implementation practice, or pedagogy materially changes. Verification method: direct_pmc_page_review. Claim scope: Supports step-by-step active-inference pedagogy and empirical-data modeling caveats; does not transfer automatically to intelligence-agent performance claims. Stakeholder role: learner, theory instructor, method reviewer. Assurance use: active-inference tutorial review, implementation-analogy caveat, and learner-facing theory learning support. Rights dimension: scientific transparency, learner comprehension, accessibility, and non-overclaiming. Direct PMC source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Shah et al. Large language models and disinformation: A double-edged sword, 2024c. URL https://ieeexplore.ieee.org/document/10540581/. IEEE article on large language models and disinformation, routed as risk-and-defense context with explicit no-generation and no-campaign boundaries. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: cognitive_influence_security. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: IEEE record, LLM disinformation literature, detection methods, or policy guidance materially changes. Verification method: script_http_200_scholarly_page_review. Claim scope: Supports bounded discussion of LLMs as both disinformation risks and defensive tools; does not authorize generation of deceptive content or manipulation campaigns. Stakeholder role: cognitive-security reviewer, AI safety reviewer, instructor. Assurance use: LLM disinformation risk review, model-misuse caveats, and defensive detection limits. Rights dimension: information integrity, democratic trust, transparency, privacy, and non-manipulative education. Direct IEEE source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Uchendu et al. Fighting fire with fire: Using large language models to combat disinformation, 2023c. URL https://aclanthology.org/2023.emnlp-main.883.pdf. ACL EMNLP paper on using large language models for disinformation detection, routed as defensive method evidence with explicit reliability and rights caveats. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: cognitive_influence_security. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: ACL Anthology PDF, detection benchmark literature, LLM model changes, or method limitations materially changes. Verification method: script_http_200_scholarly_pdf_review. Claim scope: Supports bounded discussion of using LLMs for defensive disinformation detection; does not establish universal detection reliability or endorse automated moderation. Stakeholder role: AI evaluator, cognitive-security reviewer, instructor. Assurance use: LLM-based disinformation detection caveat, defensive NLP review, and method-limit discussion. Rights dimension: free expression, transparency, fairness, accountable moderation, and detection-limit communication. Direct ACL Anthology PDF URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Wasil et al. Ai emergency preparedness, 2024d. URL https://arxiv.org/abs/2407.17347. arXiv preprint on AI emergency preparedness, routed to agent incident-response and publication-readiness caveats for tabletop exercises. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: agent_incident_response. Source tier: scholarly_preprint. Refresh cadence: semiannual. Refresh trigger: arXiv version, AI incident-preparedness literature, public-sector guidance, or risk taxonomy materially changes. Verification method: direct_arxiv_page_review. Claim scope: Supports bounded discussion of emergency preparedness for AI incidents; treated as preprint context for readiness planning, not settled policy or AGEINT incident-response evidence. Stakeholder role: incident commander, AI governance reviewer, instructor, tabletop facilitator. Assurance use: AI emergency-preparedness tabletop caveat, incident-readiness review, and public-safety boundary setting. Rights dimension: public safety, accountability, transparency, due process, and incident learning. Direct arXiv source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Williams et al. Large language models can generate election disinformation, 2025c. URL https://pmc.ncbi.nlm.nih.gov/articles/PMC11913289/. Open-access PMC article on LLM-generated election disinformation, routed as public-impact evidence for defensive cognitive-security education. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: cognitive_influence_security. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: PMC record, election-disinformation literature, LLM detection evidence, or policy context materially changes. Verification method: direct_pmc_page_review. Claim scope: Supports bounded empirical discussion of LLM-generated election disinformation risk; AGEINT uses it for detection and governance caveats, not for content generation. Stakeholder role: cognitive-security reviewer, election-integrity educator, AI governance reviewer. Assurance use: election-disinformation caveat, LLM risk boundary, and public-impact review. Rights dimension: democratic participation, information integrity, transparency, and public trust. Direct PMC source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Farid and Bohacek. Protecting world leaders against deep fakes, 2022. URL https://pmc.ncbi.nlm.nih.gov/articles/PMC9860138/. Open-access PMC article on protecting world leaders against deepfakes, routed as identity-integrity and provenance-risk support for defensive education. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: synthetic_media_provenance. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: PMC record, deepfake detection/protection literature, synthetic-media policy, or threat landscape materially changes. Verification method: direct_pmc_page_review. Claim scope: Supports bounded discussion of protecting public figures against deepfakes and synthetic impersonation; excludes identity-attack methods and targeting guidance. Stakeholder role: cognitive-security reviewer, communications reviewer, instructor. Assurance use: deepfake-protection caveat, public-figure identity risk review, and synthetic-media provenance safeguards. Rights

dimension: identity integrity, consent, democratic trust, public safety, and non-manipulative education. Direct PMC source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Coalition for Content Provenance and Authenticity. C2pa specifications, 2026. URL https://spec.c2pa.org/specifications/. C2PA specifications source for content credentials, provenance manifests, assertions, signing, verification, and media authenticity evidence. Checked as of 2026-06-06. Citation role: curriculum_anchor. Source lane: model_data_provenance. Source tier: technical_standard. Refresh cadence: semiannual. Refresh trigger: C2PA specification version, assertion vocabulary, verification model, or threat update. Verification method: direct_standards_page_review. Claim scope: content provenance, authenticity metadata, media evidence, and chain-of-custody discussion. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use; URL refreshed 2026-06-06 after liveness check.

European Union Agency for Cybersecurity. Artificial intelligence cybersecurity challenges, 2020. URL https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges. ENISA AI cybersecurity report mapping AI lifecycle assets, threat landscape, supply-chain concerns, security controls, and data-protection needs. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: ai_red_team_assurance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: ENISA AI threat landscape, AI cybersecurity guidance, or EU cybersecurity policy changes. Verification method: direct_official_page_review. Claim scope: AI cybersecurity assurance, lifecycle threat mapping, supply-chain review, and control selection. Stakeholder role: security reviewer, vendor assessor, instructor, and system steward. Assurance use: AI threat-model critique and red-team assurance checklist. Rights dimension: secure AI, data protection, trustworthiness, and supply-chain accountability. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

European Union Agency for Cybersecurity. Enisa threat landscape 2024, ENISA. URL https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024. Verified official primary source for cyber_threat_intelligence; routed to Cyber Intelligence Fundamentals; Advanced Persistent Threats; ICS/OT Security; Threat Intelligence Sharing. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: cyber_threat_intelligence. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for cyber_threat_intelligence materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of cyber_threat_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that cyber_threat_intelligence claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_enisa_threat_landscape_2024 retained.

Centers for Disease Control and Prevention. Considerations for agentic research in public health, 2026. URL https://www.cdc.gov/ai/resources/considerations-for-agentic-research-in-public-health.html. Official public-health guidance for scoping agentic research, human oversight, expert validation, sensitive-data avoidance, and non-replacement of professional judgment. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: agentic_ai_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Organisation for Economic Co-operation and Development. Towards a common reporting framework for ai incidents, 2025a. URL https://www.oecd.org/en/publications/towards-a-common-reporting-framework-for-ai-incidents_f326d4ac-en.html. OECD policy paper proposing a common AI incident reporting framework for jurisdictions and sectors, including criteria for impact and risk characterization. Checked as of 2026-05-24. Citation role: curriculum_anchor. Source lane: agent_incident_response. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: OECD AI incident reporting framework, criteria, DOI landing page, implementation, or interoperable incident-reporting guidance changes. Verification method: direct_official_page_review. Claim scope: common AI incident reporting framework, 29 reporting criteria, interoperability, high-risk systems, impact assessment, and emerging-risk review. Stakeholder role: AI incident lead, assurance reviewer, policy analyst, instructor, and learner. Assurance use: AI incident reporting template, classification checklist, impact review, and lessons-learned loop. Rights dimension: safety, accountability, impact transparency, redress evidence, cross-border interoperability, and harm learning. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Organisation for Economic Co-operation and Development. Governing with artificial intelligence: The state of play and way forward in core government functions, 2025b. URL https://www.oecd.org/en/publications/2025/06/governing-with-artificial-intelligence_398fa287/full-report/enablers-guardrails-and-engagement-for-unlocking-trustworthy-ai_2f817983.html. OECD public-sector AI governance report framing enablers, guardrails, and engagement for trustworthy AI in government. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: public_sector_transparency. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: OECD government AI governance, enabler, guardrail, engagement, or public-sector use-case update. Verification method: direct_official_page_review. Claim scope: public-sector AI governance, guardrails, engagement, transparency, and trustworthy service delivery. Stakeholder role: public-sector steward, policy reviewer, service designer, instructor, and learner. Assurance use: public-sector AI guardrail and transparency crosswalk. Rights dimension: public trust, accountability, transparency, inclusion, service quality, and citizen-facing safeguards. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Organisation for Economic Co-operation and Development. The agentic ai landscape and its conceptual foundations, 2026a. URL https://www.oecd.org/en/publications/the-agentic-ai-landscape-and-its-conceptual-foundations_396cf758-en.html. OECD AI paper clarifying the agentic AI landscape and conceptual foundations by comparing definitions and mapping shared features to the OECD AI system definition. Checked as of 2026-06-11. Citation role: curriculum_anchor. Source lane: agent_interoperability_standards. Source tier: official_policy_analysis. Refresh cadence: semiannual. Refresh trigger: OECD agentic AI paper, definition update, policy analysis, uptake data, or OECD AI-system definition guidance changes. Verification method: direct_official_page_review. Claim scope: OECD expert analysis of agentic AI definitions, frequently cited features, conceptual foundations, uptake trends, and mapping to the OECD AI system definition. Stakeholder role: policy analyst, standards steward, curriculum maintainer, instructor, and learner. Assurance use: agentic AI definition crosswalk, standards landscape map, policy-neutral concept boundary, and adoption-trend caveat review. Rights dimension: conceptual clarity, public-policy coherence, transparent terminology, accountability, and bounded claims about agentic capability. Direct OECD publication page verified live 2026-06-11; abstract describes definition comparison, OECD AI-system mapping, and uptake trends.

Organisation for Economic Co-operation and Development. Ai risks and incidents, 2026b. URL https://www.oecd.org/en/topics/ai-risks-and-incidents. OECD topic page on AI risks and incidents, including AI incident monitoring, hazard evidence, and the need for common incident reporting. Checked as of 2026-05-24. Citation role: curriculum_anchor. Source lane: agent_incident_response. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: OECD AI incident monitor, risk taxonomy, AI incident topic, or AI hazard reporting changes. Verification method: direct_official_page_review. Claim scope: AI risks, incidents, hazards, incident monitoring, accountable risk management, and cross-jurisdictional learning. Stakeholder role: incident reviewer, AI risk owner, instructor, policy analyst, and learner. Assurance use: AI incident monitor review, risk pattern briefing, incident taxonomy, and debrief evidence. Rights dimension: safety, security, privacy, discrimination, accountability, workplace rights, and public trust. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Bank for International Settlements. Fintech and the digital transformation of financial services, 2021. URL https://www.bis.org/publ/bppdf/bispap117.htm. Official BIS policy source for financial technology, market structure, data, network effects, regulation, privacy, and stability tradeoffs. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: financial_economic_security. Source tier: official_primary.

Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

European Union Agency for Network and Information Security. Protecting industrial control systems: Recommendations for europe and member states, ENISA. URL https://www.enisa.europa.eu/publications/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states. Verified official primary source for ics_ot_security_standards; routed to ICS/OT Security; Critical Infrastructure Protection; MITRE ATT&CK for ICS context. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: ics_ot_security_standards. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for ics_ot_security_standards materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of ics_ot_security_standards and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that ics_ot_security_standards claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_enisa_protecting_ics_2011 retained; stale or indirect proposal URL replaced with direct source record.

Center for Security and Emerging Technology. Adversarial machine learning and cybersecurity, 2022. URL https://cset.georgetown.edu/publication/adversarial-machine-learning-and-cybersecurity/. CSET policy-research source on adversarial machine learning and cybersecurity, used to connect AI model robustness, defensive assurance, and cyber threat-intelligence review. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: ai_red_team_assurance. Source tier: public_domain_primary. Refresh cadence: annual. Refresh trigger: CSET report URL, adversarial-ML taxonomy, cybersecurity guidance, or AI assurance practice materially changes. Verification method: direct_policy_report_page_review. Claim scope: Supports defensive framing for adversarial machine learning and cybersecurity governance; does not provide exploit, evasion, or bypass instructions. Stakeholder role: AI security reviewer, cyber analyst, instructor, red-team reviewer. Assurance use: adversarial-ML threat-model review, defensive cyber-AI control mapping, and AI assurance caveats. Rights dimension: system integrity, safety, defensive security, accountability, and public trust. Direct CSET source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Geneva Centre for Security Policy. Enhancing cognitive security and societal resilience to counter cognitive warfare, 2025. URL https://www.gcsp.ch/publications/enhancing-cognitive-security-and-societal-resilience-counter-cognitive-warfare. Policy-scholarship source for cognitive security, information literacy, critical thinking, and whole-of-society resilience. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: cognitive_influence_security. Source tier: scholarly_policy. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

International Organization for Standardization. Iso 19157:2013 geographic information - data quality, 2013. URL https://www.iso.org/standard/32575.html. International geospatial data-quality standard for completeness, logical consistency, positional accuracy, temporal quality, and usability framing. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: osint_geoint. Source tier: international_standard. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

International Organization for Standardization. Iso/iec tr 24028:2020 artificial intelligence trustworthiness overview, 2020. URL https://www.iso.org/standard/77608.html. ISO technical report page for AI trustworthiness terminology, approaches, engineering considerations, and governance vocabulary. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: ai_conformity_compliance. Source tier: international_standard. Refresh cadence: annual. Refresh trigger: ISO lifecycle stage, replacement, amendment, or JTC 1/SC 42 status changes. Verification method: direct_standards_page_review. Claim scope: trustworthy AI terminology, assurance vocabulary, and standards-aligned governance framing. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

International Organization for Standardization. Iso/iec 23894:2023 artificial intelligence guidance on risk management, 2023a. URL https://www.iso.org/standard/77304.html. International guidance for integrating AI-specific risk management into organizational activities, products, systems, and services. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: ai_ethics_data_governance. Source tier: international_standard. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

International Organization for Standardization. Iso/iec 42001:2023 artificial intelligence management system, 2023b. URL https://www.iso.org/standard/42001. International AI management-system standard for responsible AI governance, traceability, transparency, risk, and continual improvement. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: ai_ethics_data_governance. Source tier: international_standard. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

International Organization for Standardization. Iso/iec 42005:2025 ai system impact assessment, 2025. URL https://www.iso.org/standard/44545.html. ISO standard page for AI system impact assessment across lifecycle, stakeholder impact documentation, transparency, and accountability. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: ai_conformity_compliance. Source tier: international_standard. Refresh cadence: semiannual. Refresh trigger: ISO edition, corrigendum, lifecycle status, or linked package metadata changes. Verification method: direct_standards_page_review. Claim scope: AI impact-assessment workflow, stakeholder impact documentation, and accountability evidence. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Center for Strategic and International Studies. Crossing the deepfake rubicon, 2022. URL https://www.csis.org/analysis/crossing-deepfake-rubicon. CSIS public analysis on deepfake risk as a policy and security concern, routed to synthetic-media provenance and cognitive-security safeguards. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: synthetic_media_provenance. Source tier: public_domain_primary. Refresh cadence: annual. Refresh trigger: CSIS page URL, synthetic-media policy landscape, or deepfake threat assessment materially changes. Verification method: direct_policy_page_review. Claim scope: Supports bounded policy discussion of deepfake risk and governance; does not provide impersonation, targeting, or manipulation instructions. Stakeholder role: cognitive-security reviewer, policy analyst, instructor. Assurance use: deepfake risk governance, policy brief caveats, and synthetic-media threat-boundary review. Rights dimension: identity integrity, public trust, consent, democratic resilience, and non-manipulative education. Direct CSIS source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Central Intelligence Agency Center for the Study of Intelligence. Sherman kent's final thoughts on analyst-policymaker relations, 1994. URL https://www.cia.gov/resources/csi/static/Kent-Final-Thoughts-Analyst-Policymaker-Relations.pdf. Official CIA CSI republication of Kent's final essay on analyst-policy relations, warning, intention, and communication boundaries. Checked as of 2026-06-11. Citation role: curriculum_anchor. Source lane: analytic_tradecraft_evidence. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: Refresh if CIA replaces the

PDF or publishes a newer CSI version. Verification method: direct_pdf_download. Claim scope: Supports bounded claims about analyst-policy communication and warning-intelligence responsibilities. Stakeholder role: analytic tradecraft instructor; policy liaison; analyst supervisor. Assurance use: Keeps warning and policy-support lessons inside advisory rather than decision-authority claims. Rights dimension: public-domain government source; cite as historical context. Direct CIA PDF verified live 2026-06-11; use for warning and analyst-policy boundary framing.

Central Intelligence Agency Center for the Study of Intelligence. Sherman kent and the profession of intelligence analysis, 2002. URL https://www.cia.gov/resources/csi/static/Kent-Profession-Intel-Analysis.pdf. Official CIA Center for the Study of Intelligence essay on Kent's professionalization of intelligence analysis and analytic standards. Checked as of 2026-06-11. Citation role: curriculum_anchor. Source lane: analytic_tradecraft_evidence. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: Refresh if CIA replaces the PDF or publishes a newer CSI Kent/tradecraft history. Verification method: direct_pdf_download. Claim scope: Supports claims about Kent's role in professional analytic standards and intelligence-analysis identity. Stakeholder role: curriculum designer; analytic tradecraft instructor; analyst supervisor. Assurance use: Grounds professional-standards framing for tradecraft lessons. Rights dimension: public-domain government source; cite as historical context. Direct CIA PDF verified live 2026-06-11; use for Kent-as-profession and standards claims, not for contemporary agency policy.

Financial Action Task Force. Updated guidance for a risk-based approach to virtual assets and virtual asset service providers, 2021. URL https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html. Official FATF guidance for virtual-asset risk, VASP supervision, travel-rule compliance, and non-evasion FININT education. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: financial_economic_security. Source tier: international_standard. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Financial Action Task Force. The fatf recommendations, 2025. URL https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html. Official international AML/CFT/CPF standard for risk-based controls, beneficial ownership, information sharing, supervision, and mutual evaluation. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: financial_economic_security. Source tier: international_standard. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Internet Engineering Task Force. Rfc 9110: Http semantics, 2022. URL https://www.rfc-editor.org/rfc/rfc9110.html. IETF standard for HTTP semantics used to ground API contracts, methods, status codes, content negotiation, and safe integration language. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: agent_interoperability_standards. Source tier: internet_standard. Refresh cadence: annual. Refresh trigger: RFC update, errata, bis document, or HTTP specification status changes. Verification method: direct_standards_page_review. Claim scope: API semantics, tool-interface constraints, status handling, and integration contracts. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

U.S. National Science Foundation. Advancing artificial intelligence agent ecosystems through the nsf pesose program, 2026. URL https://www.nsf.gov/funding/opportunities/dcl-advancing-artificial-intelligence-ai-agent-ecosystems. Official NSF source for open AI-agent protocol ecosystems, interoperability, identity, access control, auditability, and safe message formats. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: agentic_ai_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

FitzGerald T. Rigoli F. Schwartenbeck P. & Pezzulo G. Friston, K. Active inference: A process theory, 2017. URL https://direct.mit.edu/neco/article/29/1/1/8207/Active-Inference-A-Process-Theory. Formalizes active inference as a process theory in which belief updating proceeds by gradient descent on variational free energy and policies are selected by minimizing expected free energy over a Markov decision process generative model. Checked as of 2026-06-08. Citation role: curriculum_anchor. Source lane: cognitive_active_inference. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: source URL, DOI, edition/standard version, or claim scope materially changes. Verification method: direct_source_url_review. Claim scope: Lessons 2 & 4 - belief updating, policy selection, and expected free energy as the action-selection objective. Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.

K. Friston. The free-energy principle: a unified brain theory?, 2010. URL https://www.nature.com/articles/nrn2787. Karl Friston's flagship review introducing the free-energy principle, showing how a variational free-energy functional provides a tractable upper bound on surprise (negative log model evidence) that the brain minimizes through perception and action. Checked as of 2026-06-08. Citation role: curriculum_anchor. Source lane: cognitive_active_inference. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: source URL, DOI, edition/standard version, or claim scope materially changes. Verification method: direct_source_url_review. Claim scope: Lesson 1 'Active Inference and AGEINT' - the claim that variational free energy bounds surprise, providing the primary source behind a treatment previously grounded in a bachelor's thesis. Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.

Office of Management General Services Administration, Budget, and CDO Council. Federal data strategy, 2026. URL https://strategy.data.gov/. Official federal data-governance benchmark for data as a strategic asset, ethical governance, lifecycle practices, and learning culture. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: ai_ethics_data_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

World Bank GovTech and Public Sector Innovation Global Team. Artificial intelligence working group, 2026. URL https://www.worldbank.org/en/programs/govtech/artificial-intelligence. Official World Bank GovTech source for public-sector AI policy instruments, implementation knowledge exchange, and inclusive government capacity. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: public_sector_agentic_ai. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: working-group membership, policy instrument, repository, or public-sector case update. Verification method: direct_official_page_review. Claim scope: public-sector AI implementation, GovTech capacity, inclusive services, and institutional governance. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Cynthia M. Grabo. Handbook of warning intelligence, 1972. URL https://www.cia.gov/readingroom/docs/CIA-RDP80B00829A000800040001-6.pdf. CIA Reading Room declassified warning-intelligence handbook volume used for indications-and-warning concepts. Checked as of 2026-06-11. Citation role: curriculum_anchor. Source lane: warning_intelligence. Source tier: official_declassified_primary. Refresh cadence: annual. Refresh trigger: Refresh if CIA Reading Room record or declassification file changes. Verification method: direct_pdf_download. Claim scope: Supports claims about indications, warning, assumptions, and uncertainty in historical warning practice. Stakeholder role: analytic tradecraft instructor; warning-methods reviewer. Assurance use: Adds source-backed warning vocabulary while preserving evidence-bounded educational boundaries. Rights dimension: declassified public government record; avoid operationalizing historical procedures. CIA Reading Room PDF verified live 2026-06-11; use for historical warning concepts, not operational collection instructions.

International AI Safety Report Writing Group and Expert Advisory Panel. International ai safety report 2026, 2026. URL https://internationalaisafetyreport.org/publication/international-ai-safety-report-2026. International AI Safety Report 2026 chaired by Yoshua Bengio with an

international expert advisory panel; used as a synthesis source for advanced-AI safety evidence and uncertainty, not as a policy endorsement. Checked as of 2026-06-12. Citation role: curriculum_anchor. Source lane: assurance_evaluation_evidence. Source tier: official_scientific_synthesis. Refresh cadence: annual. Refresh trigger: International AI Safety Report release, extended policymaker summary, expert advisory panel update, or major frontier-AI safety evidence changes. Verification method: direct_official_page_review. Claim scope: international advanced-AI safety evidence, risk-taxonomy synthesis, capability and impact assessment, and policy-neutral scientific uncertainty framing. Stakeholder role: assurance evaluator, policy reviewer, instructor, system steward, and learner. Assurance use: advanced-AI safety evidence review, uncertainty register, capability-risk synthesis, and policy-neutral assurance briefing. Rights dimension: safety, accountability, transparency, uncertainty communication, international coordination, and harm prevention. Direct official report landing page verified live (HTTP 200, International AI Safety Report 2026 page on-topic); the official PDF and arXiv record remain secondary evidence when needed.

Lars C. Borg; Kristian C. Gustafson. Teaching structured analytic techniques across nations: Same, same but different, 2025. URL https://doi.org/10.1080/08850607.2025.2479991. Peer-reviewed article on cross-national SAT teaching used for pedagogy, transfer, and local-context caveats. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: analytic_method_pedagogy. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: Publisher metadata, DOI record, correction, or retraction status changes. Verification method: crossref_doi_metadata_review. Claim scope: Supports bounded claims about SAT teaching across institutional and national contexts without assuming one curriculum design transfers unchanged. Stakeholder role: curriculum designer; analytic tradecraft instructor; pedagogy reviewer. Assurance use: Strengthens AGEINT's classroom framing and local-context caveats for SAT exercises. Rights dimension: copyrighted scholarly article; cite DOI metadata and summarize sparingly. Crossref DOI metadata verified live 2026-06-15 for title, authors, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.

Norman Dalkey; Olaf Helmer. An experimental application of the delphi method to the use of experts, 1963. URL https://doi.org/10.1287/mnsc.9.3.458. Classic peer-reviewed Delphi-method article used as historical method context for structured expert elicitation and iterative judgment aggregation. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: forecasting_calibration_evidence. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: Publisher metadata, DOI record, correction, or retraction status changes. Verification method: crossref_doi_metadata_review. Claim scope: Supports bounded claims about Delphi as an expert-elicitation and judgment-aggregation technique, not proof that expert panels converge on truth. Stakeholder role: forecasting instructor; methods instructor; curriculum designer. Assurance use: Adds historical method roots for aggregation and structured elicitation exercises. Rights dimension: copyrighted scholarly article; cite DOI metadata and summarize sparingly. Crossref DOI metadata verified live 2026-06-15 for title, authors, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.

Frank G. Hoffman. Conflict in the 21st century: The rise of hybrid wars (potomac institute, 2007), 2007. URL https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf. Verified scholarly repository record source for hybrid_warfare_doctrine; routed to Gray Zone / Hybrid Warfare / Non-State Actor Intelligence / Irregular Warfare. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: hybrid_warfare_doctrine. Source tier: scholarly_repository_record. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for hybrid_warfare_doctrine materially changes. Verification method: direct_source_url_review. Claim scope: Supports bounded AGEINT discussion of hybrid_warfare_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that hybrid_warfare_doctrine claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_hoffman_2007_hybrid_wars retained.

Cloppert M. J. & Amin R. M. Hutchins, E. M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains, 2011. URL https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf. Verified professional documentation source for cyber_threat_intelligence; routed to Cyber Intelligence Fundamentals; APT Threat Intelligence; Structured Analytic Techniques for Cyber. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: cyber_threat_intelligence. Source tier: professional_documentation. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for cyber_threat_intelligence materially changes. Verification method: direct_source_url_review. Claim scope: Supports bounded AGEINT discussion of cyber_threat_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that cyber_threat_intelligence claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_hutchins_2011_kill_chain normalized to professional_hutchins_2011_kill_chain.

E-ISAC & SANS ICS. Ics defense use case no. 6: Modular ics malware, 2017. URL https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt4f6cc0b6358c6883/607f235a6371c75a11ad9f5a/E-ISAC_SANS_Ukraine_DUC_6.pdf. Verified official primary source for historical_ics_incidents; routed to Historical ICS Cyber Incidents; ICS/OT Security; MITRE ATT&CK for ICS. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: historical_ics_incidents. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for historical_ics_incidents materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of historical_ics_incidents and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that historical_ics_incidents claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_nerc_eisac_ukraine_duc6_2017 retained.

ICS-CERT. Icsa-10-272-01: Stuxnet malware mitigation, 2010. URL https://www.cisa.gov/uscert/ics/advisories/ICSA-10-272-01. Verified official primary source for historical_ics_incidents; routed to Historical ICS Cyber Incidents; ICS/OT Security; MITRE ATT&CK for ICS. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: historical_ics_incidents. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for historical_ics_incidents materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of historical_ics_incidents and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that historical_ics_incidents claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_cisa_isc_cert_stuxnet_advisory retained.

IETF. Rfc 9449: Oauth 2.0 demonstrating proof of possession, 2023. URL https://www.rfc-editor.org/rfc/rfc9449.html. Internet standard for sender-constrained OAuth tokens, useful for agent tool-call identity and credential-binding discussions. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: agentic_ai_governance. Source tier: internet_standard. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding

and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

IETF. Rfc 9700: Best current practice for oauth 2.0 security, 2025. URL https://www.rfc-editor.org/rfc/rfc9700.html. Internet standards-track security guidance for OAuth deployment, token protection, redirect safety, and authorization hardening. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: agentic_ai_governance. Source tier: internet_standard. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

in-toto Project. in-toto, 2026. URL https://in-toto.io/. in-toto framework for securing software supply-chain integrity with verifiable metadata and attestations; used to ground release-chain evidence and provenance checks. Checked as of 2026-06-06. Citation role: curriculum_anchor. Source lane: secure_release_change_control. Source tier: security_standard. Refresh cadence: quarterly. Refresh trigger: in-toto specification, attestation format, layout model, supply-chain integration, or provenance tooling changes. Verification method: direct_project_page_review. Claim scope: software supply-chain layout, signed attestations, step-level integrity, artifact provenance, and verifiable release workflow evidence. Stakeholder role: release engineer, provenance reviewer, assurance evaluator, instructor, and learner. Assurance use: attestation-chain review, provenance evidence package, release-step integrity check, and supplier handoff audit. Rights dimension: security, provenance, accountability, auditability, and user protection. Direct source URL verified live (HTTP 200, official in-toto project page) for AGEINT curriculum use.

Cloud Security Alliance AI Safety Initiative. Csa research note: Nist ai agent red-teaming standards (march 2026), 2026a. URL https://labs.cloudsecurityalliance.org/research/csa-research-note-nist-ai-agent-red-teaming-standards-202603/. CSA research note on NIST AI agent red-teaming standards summarizing CAISI findings and recommended adversarial-ML testing protocols; reported success-rate figures treated as ESTIMATE. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: ai_red_team_assurance. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: CSA/NIST AI agent red-teaming standards note revisions, CAISI findings, adversarial-ML taxonomy, or red-team standard updates. Verification method: direct_official_page_review. Claim scope: NIST AI agent red-teaming standards, adversarial-ML taxonomy, indirect prompt-injection and memory-poisoning test scenarios, and enterprise compliance. Stakeholder role: red-team reviewer, assurance evaluator, instructor, compliance officer, and learner. Assurance use: AI red-team standards crosswalk, adversarial-ML test scope, multi-attempt evaluation plan, and enterprise compliance review. Rights dimension: security, accountability, validity, reliability, transparency, and trustworthy AI assurance. Direct source URL verified live (HTTP 200, on-topic CSA/NIST AI agent red-teaming standards note) for AGEINT curriculum use.

OpenAPI Initiative. Openapi specification, 2026b. URL https://spec.openapis.org/oas/. Official OpenAPI specification index for describing HTTP APIs, schemas, operations, errors, and contract validation. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: agent_interoperability_standards. Source tier: open_standard. Refresh cadence: semiannual. Refresh trigger: OpenAPI version, schema revision, or specification publication changes. Verification method: direct_standards_page_review. Claim scope: API contract design, schema validation, tool-call description, and integration evidence. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

OWASP Gen AI Security Project (Agentic Security Initiative). Agentic ai - threats and mitigations, 2025. URL https://genai.owasp.org/resource/agentic-ai-threats-and-mitigations/. OWASP Agentic Security Initiative threat-model-based reference of emerging agentic AI threats and mitigations; standards-body guidance for defensive curriculum use. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: ai_red_team_assurance. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: OWASP Agentic Security Initiative whitepaper revisions, threat-model updates, or new agentic threats-and-mitigations guidance changes. Verification method: direct_official_page_review. Claim scope: agentic AI threats and mitigations, threat-model-based reference, and OWASP Agentic Security Initiative mitigation baseline. Stakeholder role: red-team reviewer, threat modeler, instructor, system steward, and learner. Assurance use: agentic threat-model reference, mitigation baseline checklist, red-team scope guide, and ASI-aligned assurance review. Rights dimension: security, accountability, transparency, and trustworthy AI assurance. Direct source URL verified live (HTTP 200, on-topic OWASP agentic threats-and-mitigations resource) for AGEINT curriculum use.

World Wide Web Consortium Web Accessibility Initiative. Wcag 2 overview, 2026c. URL https://www.w3.org/WAI/standards-guidelines/wcag/. W3C WAI overview for WCAG 2.0, 2.1, and 2.2 conformance, success criteria, and accessibility standard selection in digital curriculum artifacts. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: accessibility_digital_inclusion. Source tier: technical_standard. Refresh cadence: semiannual. Refresh trigger: WCAG publication, conformance guidance, or public-sector accessibility requirement changes. Verification method: direct_standards_page_review. Claim scope: web accessibility, conformance checks, inclusive digital artifacts, and WCAG-aligned review. Stakeholder role: learner, instructor, public-sector service user, and accessibility reviewer. Assurance use: accessibility acceptance criteria and remediation evidence. Rights dimension: disability access, equal participation, and digital inclusion. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Intelligence.gov. About this site, 2026a. URL https://www.intelligence.gov/about. Intelligence.gov public page explaining the site as an IC transparency platform and public front door. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: ic_public_transparency. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: Intelligence.gov page content, URL, or transparency-platform framing materially changes. Verification method: browser_fetch_official_html_review. Claim scope: public transparency-platform context for orientation and publication-readiness posture. Stakeholder role: learner, instructor, publication reviewer. Assurance use: anchors public-facing transparency language used in AGEINT release-surface checks. Rights dimension: public education page used for transparency and public-readiness framing. Direct URL verified on 2026-06-14 through browser fetch because intelligence.gov returned 403 to plain curl; fetched HTML title and page content matched the About This Site page.

Intelligence.gov. Our values: Accountability, 2026b. URL https://www.intelligence.gov/mission/our-values/accountability. Intelligence.gov public values page describing IC accountability, lawfulness, oversight, and civil liberties framing. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: ic_public_transparency. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: Intelligence.gov page content, URL, or public values framing materially changes. Verification method: browser_fetch_official_html_review. Claim scope: public accountability and oversight context for legal/ethical framing. Stakeholder role: learner, instructor, civil-liberties reviewer. Assurance use: anchors public-facing accountability language and oversight explanations. Rights dimension: public education page used for rights, accountability, and oversight framing. Direct URL verified on 2026-06-14 through browser fetch because intelligence.gov returned 403 to plain curl; fetched HTML title and page content matched the accountability page.

Intelligence.gov. Our values: Collaboration, 2026c. URL https://www.intelligence.gov/mission/our-values/collaboration. Intelligence.gov public values page describing collaboration across IC elements and external partners. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: ic_public_transparency. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: Intelligence.gov page content, URL, or public values framing materially changes. Verification method: browser_fetch_official_html_review. Claim scope: public collaboration context for modular handoff, partner engagement, and source-pack routing. Stakeholder role: learner, instructor, reviewer. Assurance use: supports modular substrate language about collaboration without implying live liaison or tasking. Rights dimension: public education page used for orientation and governance framing. Direct URL verified on 2026-06-14 through browser fetch because intelligence.gov returned 403 to plain curl; fetched HTML title and page content matched the collaboration page.

Intelligence.gov. Our values: Innovation, 2026d. URL https://www.intelligence.gov/mission/our-values/innovation. Intelligence.gov public values page describing innovation as more than technology and tying it to mission needs. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: ic_public_transparency. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: Intelligence.gov page content, URL, or public values framing materially changes. Verification method: browser_fetch_official_html_review. Claim scope: public innovation context for bounded agentic assistance and technology-governance framing. Stakeholder role: learner, instructor, innovation reviewer. Assurance use: keeps innovation claims tied to public IC values rather than unchecked automation. Rights dimension: public education page used for orientation and technology-governance framing. Direct URL verified on 2026-06-14 through browser fetch because intelligence.gov returned 403 to plain curl; fetched HTML title and page content matched the innovation page.

Intelligence.gov. Mission, 2026e. URL https://www.intelligence.gov/mission. Intelligence.gov public mission page describing the IC mission, customers, and values at a high level. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: ic_public_transparency. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: Intelligence.gov page content, URL, or public mission framing materially changes. Verification method: browser_fetch_official_html_review. Claim scope: public mission and values context for reader-facing IC orientation. Stakeholder role: learner, instructor, reviewer. Assurance use: anchors introductory IC mission language to the public official portal. Rights dimension: public education page used for orientation and transparency framing. Direct URL verified on 2026-06-14 through browser fetch because intelligence.gov returned 403 to plain curl; fetched HTML title and page content matched the mission page.

Intelligence.gov. Our values: Transparency, 2026f. URL https://www.intelligence.gov/mission/our-values/transparency. Intelligence.gov public values page describing transparency principles, public understanding, and protection of sources and methods. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: ic_public_transparency. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: Intelligence.gov page content, URL, or public values framing materially changes. Verification method: browser_fetch_official_html_review. Claim scope: public transparency context for release, public understanding, and source-protection boundaries. Stakeholder role: learner, instructor, transparency reviewer. Assurance use: supports transparent manuscript and evidence-packet posture without exposing sources or methods. Rights dimension: public education page used for transparency and public-trust framing. Direct URL verified on 2026-06-14 through browser fetch because intelligence.gov returned 403 to plain curl; fetched HTML title and page content matched the transparency page.

Irving L. Janis. Groupthink: Psychological studies of policy decisions and fiascoes, 1982. URL https://books.google.com/books/about/Groupthink.html?id=ZB0bAAAAIAAJ. Scholarly book record for Janis's groupthink model used as classic context for dissent, alternatives, and group-decision failure claims. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: analytic_cognition_and_bias. Source tier: scholarly_book_metadata. Refresh cadence: annual. Refresh trigger: Bibliographic metadata, edition record, or accessible publisher record changes. Verification method: bibliographic_metadata_review. Claim scope: Supports bounded classic groupthink and dissent-context framing, not a validated claim that one checklist eliminates group decision failure. Stakeholder role: analytic tradecraft instructor; cognition reviewer; curriculum designer. Assurance use: Keeps group-process lessons tied to a named scholarly source while preserving caveats about retrospective failure explanation. Rights dimension: copyrighted scholarly book metadata only; cite and summarize sparingly. Google Books bibliographic record verified live 2026-06-15 for title, author, edition, publisher, year, and ISBN metadata; used as bibliographic support because no current publisher landing page was available.

Jonathan A. W. R. Mitchell Jennifer Stromer-Galley and colleagues. Flexible versus structured support for reasoning: Enhancing analytical reasoning through a flexible analytic technique, 2020. URL https://eprints.gla.ac.uk/272733/. Scholarly record and abstract for an experimental comparison of flexible SAT support and structured/no-SAT conditions for reasoning quality. Checked as of 2026-06-11. Citation role: curriculum_anchor. Source lane: sat_evaluation_evidence. Source tier: scholarly_repository_record. Refresh cadence: annual. Refresh trigger: Refresh if repository metadata, DOI, or publisher record changes. Verification method: repository_metadata_review. Claim scope: Supports bounded claims that flexible SAT support can improve reasoning quality in a specific experimental setting. Stakeholder role: curriculum designer; analytic standards trainer; evaluation lead. Assurance use: Adds a positive but bounded empirical counterpoint to SAT critique and doctrine sources. Rights dimension: repository metadata and scholarly article; cite source and avoid extended quotation. University of Glasgow repository metadata verified live 2026-06-11; use for flexible-SAT evidence as one bounded study, not all-purpose SAT proof.

Robert Jervis. Why intelligence and policymakers clash, 2022. URL https://www.pnas.org/doi/10.1073/pnas.2116638118. PNAS perspective on intelligence-policy friction and the limits of postmortem explanations of intelligence failure. Checked as of 2026-06-11. Citation role: curriculum_anchor. Source lane: intelligence_failure_postmortem. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: Refresh if publisher metadata, correction, or retraction status changes. Verification method: publisher_metadata_review. Claim scope: Supports claims about policy-intelligence friction, hindsight bias in postmortems, and limits of simple failure narratives. Stakeholder role: curriculum designer; governance reviewer; analyst supervisor. Assurance use: Constrains postmortem lessons so they do not imply a single technique could prevent complex failure. Rights dimension: copyrighted scholarly article; cite metadata and summarize sparingly. PNAS DOI/publisher metadata verified live 2026-06-11; use for postmortem and policy-friction boundary claims.

Rob Johnston. Analytic culture in the u.s. intelligence community, 2005. URL https://www.cia.gov/resources/csi/static/Analytic-Culture-Intelligence-Community.pdf. CIA/CSI professional-literature monograph on analytic institutions, incentives, training, and cultural constraints. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: intelligence_profession_literature. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: CIA source URL, release status, or public text materially changes. Verification method: direct_official_page_and_pdf_review. Claim scope: professional-context support for analytic culture, method standardization limits, and institution-level tradecraft constraints. Stakeholder role: curriculum designer, analyst, reviewer. Assurance use: keeps culture and training claims tied to official professional context rather than slogans. Rights dimension: public professional literature used for education and review without operational tasking. Direct CIA CSI book page and static PDF URL verified on 2026-06-15; metadata updated to preserve the existing citation key while crediting the monograph author.

Beth Goldberg Steve Rathje Jon Roozenbeek, Sander van der Linden and Stephan Lewandowsky. Psychological inoculation improves resilience against misinformation on social media, 2022. URL https://www.science.org/doi/10.1126/sciadv.abo6254. Science Advances article showing that psychological inoculation campaigns on social media can improve misinformation resilience at scale under measured study conditions. Checked as of 2026-06-11. Citation role: curriculum_anchor. Source lane: cognitive_resilience_evidence. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: Science Advances record, DOI metadata, replication literature, meta-analysis, or evidence boundary materially changes. Verification method: direct_scholarly_page_review. Claim scope: Peer-reviewed Science Advances study testing psychological inoculation videos for improving misinformation resilience at scale, with bounded transfer from measured outcomes to curriculum claims. Stakeholder role: instructor, cognitive-security reviewer, learner, assurance reviewer, and affected-community representative. Assurance use: prebunking evidence boundary, inoculation mechanism caveat, outcome-measure review, and cognitive-security lesson-scope limits. Rights dimension: cognitive autonomy, transparent educational framing, anti-manipulation safeguards, measured-outcome limits, and rights-aware prebunking practice. Direct Science Advances DOI page verified live 2026-06-11 with title, journal, DOI, and abstract-level claim that inoculation campaigns improved misinformation resilience at scale.

Richards J. Heuer Jr. Psychology of intelligence analysis, 2007. URL https://www.cia.gov/resources/csi/books-monographs/psychology-of-intelligence-analysis-2/. Foundational analytic cognition source for bias, mental models, and structured reasoning. Checked as of 2026-06-06. Citation role: curriculum_anchor. Source lane: analytic_tradecraft. Source tier: scholarly_or_official. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding

and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use; URL refreshed 2026-06-06 after liveness check.

Daniel. Kahneman. Thinking, fast and slow (wikipedia), 2011. URL https://search.worldcat.org/title/Thinking-fast-and-slow/oclc/706020998. Verified scholarly book metadata source for cognitive_bias_foundations; routed to Cognitive Security (dual-process neurocognitive mechanisms); Epistemic Rigor & Analytic Tradecraft. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: cognitive_bias_foundations. Source tier: scholarly_book_metadata. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for cognitive_bias_foundations materially changes. Verification method: direct_publisher_or_catalog_record_review. Claim scope: Supports bounded AGEINT discussion of cognitive_bias_foundations and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that cognitive_bias_foundations claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_kahneman_2011_thinking_fast_slow retained; stale or indirect proposal URL replaced with direct source record.

Shailesh Mishra Christoph Endres Thorsten Holz Kai Greshake, Sahar Abdelnabi and Mario Fritz. Not what you've signed up for: Compromising real-world llm-integrated applications with indirect prompt injection, 2023. URL https://arxiv.org/abs/2302.12173. arXiv security paper showing that malicious third-party content retrieved by LLM-integrated applications can indirectly inject instructions and compromise real-world application behavior. Checked as of 2026-06-10. Citation role: curriculum_anchor. Source lane: agentic_ai_security. Source tier: scholarly_preprint. Refresh cadence: annual. Refresh trigger: arXiv record, DOI record, indirect prompt-injection literature, agentic tool-security guidance, or threat taxonomy materially changes. Verification method: direct_scholarly_page_review. Claim scope: Indirect prompt injection risk in LLM-integrated applications where retrieved or external content can alter model behavior and trigger data theft, tool misuse, or ecosystem contamination. Stakeholder role: agent builder, security reviewer, assurance reviewer, instructor, learner, and incident responder. Assurance use: agentic retrieval and tool-use security review, indirect prompt-injection threat modeling, blocked-action logging, memory-contamination checks, and human escalation evidence. Rights dimension: protects users and affected parties from hidden instruction/data blending, unauthorized disclosure, unsafe tool invocation, and contaminated downstream reuse. Direct arXiv source URL verified live 2026-06-10 with title, authors, submission and revision metadata, DOI, and abstract describing indirect prompt-injection attacks.

& Kaplan S. Kaplan, R. The experience of nature: A psychological perspective, 1989. URL https://search.worldcat.org/title/The-experience-of-nature-%3A-a-psychological-perspective/oclc/18814094. Verified scholarly book metadata source for cognitive_performance; routed to Productivity Intelligence & Cognitive Performance (attention restoration, information architecture); Cognitive Security & Inoculation appendix. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: cognitive_performance. Source tier: scholarly_book_metadata. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for cognitive_performance materially changes. Verification method: direct_publisher_or_catalog_record_review. Claim scope: Supports bounded AGEINT discussion of cognitive_performance and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that cognitive_performance claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_kaplan_kaplan_1989_attention_restoration retained; stale or indirect proposal URL replaced with direct source record.

Miller J. C. Redlich A. D. & Kleinman S. M. Kelly, C. E. A taxonomy of interrogation methods, 2013. URL https://doi.apa.org/doi/10.1037/a0030310. A peer-reviewed taxonomy organizing interrogation into macro-level approaches, six meso-level domains (rapport/relationship building, context manipulation, emotion provocation, confrontation/competition, collaboration, presentation of evidence), and micro-level techniques, providing a study-grounded vocabulary for analyzing elicitation methods rather than an operational manual. Checked as of 2026-06-08. Citation role: curriculum_anchor. Source lane: counterintelligence_source_integrity. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: source URL, DOI, edition/standard version, or claim scope materially changes. Verification method: direct_source_url_review. Claim scope: Backs the AGEINT study-taxonomy framing of interrogation/elicitation methods, signaling analytic categorization rather than an operational how-to. Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.

Gary Klein. Performing a project premortem, 2007. URL https://hbr.org/2007/09/performing-a-project-premortem. Professional practice article introducing the premortem as a structured way to surface possible failure causes before commitment. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: analytic_method_pedagogy. Source tier: professional_practice. Refresh cadence: annual. Refresh trigger: Publisher page, author metadata, or access status changes. Verification method: publisher_page_review. Claim scope: Supports bounded classroom use of premortem thinking as a failure-imagination aid, not a validated guarantee of risk detection. Stakeholder role: methods instructor; curriculum designer; reviewer. Assurance use: Adds a named structured failure-review technique while retaining explicit evidence limits. Rights dimension: copyrighted professional article; cite metadata and summarize sparingly. Harvard Business Review article page verified live 2026-06-15 for title, author, publication date, and publisher record.

Mariusz Kozera. Fitness osint: Identifying and tracking military and security personnel with fitness applications, 2020. URL https://securityanddefence.pl/Fitness-OSINT-Identifying-and-tracking-military-and-security-personnel-with-fitness,131759,0,2.html. Security and Defence article on identifying and tracking military and security personnel through fitness-app data, routed as a privacy and source-minimization warning. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: osint_geoint. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: journal article URL, fitness-app privacy literature, OSINT leakage patterns, or platform practices materially changes. Verification method: script_http_200_scholarly_page_review. Claim scope: Supports defensive discussion of fitness-app OSINT leakage and privacy risk; does not authorize tracking, doxxing, or targeting of real personnel. Stakeholder role: OSINT instructor, privacy reviewer, assurance reviewer. Assurance use: OSINT privacy-risk review, fitness-app leakage classroom caveat, and public-source minimization checklist. Rights dimension: privacy, physical safety, minimization, consent, and protection from live tracking. Direct journal source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Inc. LangChain. Langchain documentation, 2025a. URL https://docs.langchain.com. Verified professional documentation source for agentic_framework_docs; routed to LangChain/LangGraph Patterns appendix; AGEINT Python Code Library. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: agentic_framework_docs. Source tier: professional_documentation. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for agentic_framework_docs materially changes. Verification method: direct_professional_documentation_review. Claim scope: Supports bounded AGEINT discussion of agentic_framework_docs and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that agentic_framework_docs claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key professional_langchain_documentation retained.

Inc. LangChain. Langgraph documentation, 2025b. URL https://langchain-ai.github.io/langgraph/. Verified professional documentation source for agentic_framework_docs; routed to LangChain/LangGraph Patterns appendix; AGEINT Python Code Library; Frameworks & Infrastructure. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: agentic_framework_docs. Source tier: professional_documentation. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for agentic_framework_docs materially changes. Verification method: direct_professional_documentation_review. Claim scope: Supports bounded AGEINT discussion of agentic_framework_docs and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that agentic_framework_docs claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key professional_langgraph_documentation retained.

et al. Lazer, David M.J. The science of fake news (science, 2018), 2018. URL https://www.science.org/doi/10.1126/science.aao2998. Verified scholarly peer reviewed source for disinformation_misinformation_science; routed to Active Measures and Disinformation; Information Warfare and Cognitive Security; Social Engineering. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: disinformation_misinformation_science. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for disinformation_misinformation_science materially changes. Verification method: direct_source_url_review. Claim scope: Supports bounded AGEINT discussion of disinformation_misinformation_science and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that disinformation_misinformation_science claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_lazer_2018_science_fake_news retained.

Assante M. J. & Conway T. Lee, R. M. Analysis of the cyber attack on the ukrainian power grid, 2016. URL https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt6a77276749b76a40/607f235992f0063e5c070fff/E-ISAC_SANS_Ukraine_DUC_5%5B73%5D.pdf. Verified official primary source for historical_ics_incidents; routed to Historical ICS Cyber Incidents; ICS/OT Security; Threat Intelligence Sharing for Critical Infrastructure. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: historical_ics_incidents. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for historical_ics_incidents materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of historical_ics_incidents and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that historical_ics_incidents claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_eisac_sans_ukraine_2016 retained.

Donghyun Lee and Mo Tiwari. Prompt infection: Llm-to-llm prompt injection within multi-agent systems, 2024. URL https://arxiv.org/abs/2410.07283. arXiv paper documenting self-replicating LLM-to-LLM prompt injection within multi-agent systems; used as a defensive, evidence-bounded counterintelligence anchor with LLM-tagging mitigation. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: agent_incident_response. Source tier: scholarly_preprint. Refresh cadence: annual. Refresh trigger: New arXiv version of Prompt Infection, revised propagation model, or successor multi-agent injection defense research changes. Verification method: direct_scholarly_page_review. Claim scope: self-replicating prompt injection across multi-agent systems, propagation via shared memory and tool outputs, and LLM tagging defense. Stakeholder role: incident reviewer, threat modeler, instructor, system steward, and learner. Assurance use: cross-agent injection threat briefing, propagation-containment review, LLM-tagging defense map, and synthetic infection tabletop. Rights dimension: security, integrity, accountability, and harm prevention. Direct source URL verified live (HTTP 200, on-topic arXiv prompt-infection paper) for AGEINT curriculum use.

& van der Linden Sander. Lewandowsky, Stephan. Countering misinformation through inoculation and prebunking, 2021. URL https://doi.org/10.1080/10463283.2021.1876983. Verified scholarly peer reviewed source for cognitive_security_inoculation; routed to Cognitive Security (psychological inoculation & prebunking); Cognitive Security Operations. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: cognitive_security_inoculation. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for cognitive_security_inoculation materially changes. Verification method: direct_doi_record_review. Claim scope: Supports bounded AGEINT discussion of cognitive_security_inoculation and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that cognitive_security_inoculation claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_lewandowsky_vanderlinden_2021_inoculation_review retained.

Cook John Ecker Ullrich K. H. et al. Lewandowsky, Stephan. The debunking handbook 2020, 2020. URL https://digitalcommons.unl.edu/scholcom/245/. Verified scholarly repository record source for cognitive_security_inoculation; routed to Cognitive Security (psychological inoculation & prebunking); corrections and debunking protocol. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: cognitive_security_inoculation. Source tier: scholarly_repository_record. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for cognitive_security_inoculation materially changes. Verification method: direct_source_url_review. Claim scope: Supports bounded AGEINT discussion of cognitive_security_inoculation and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that cognitive_security_inoculation claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_lewandowsky_cook_2020_debunking_handbook retained.

Perez E. Piktus A. Petroni F. Karpukhin V. Goyal N. Kuttler H. Lewis M. Yih W.-t. Rocktaschel T. Riedel-S. & Kiela D. Lewis, P. Retrieval-augmented generation for knowledge-intensive nlp tasks, 2020. URL https://arxiv.org/abs/2005.11401. Verified scholarly preprint source for agentic_memory; routed to Foundations of AGEINT (agent memory); Design Patterns & Archetypes (RAG architecture); LangChain/LangGraph Patterns appendix; AGEINT Python Code Li.... AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: agentic_memory. Source tier: scholarly_preprint. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for agentic_memory materially changes. Verification method: direct_arxiv_record_review. Claim scope: Supports bounded AGEINT discussion of agentic_memory and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that agentic_memory claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_lewis_2020_rag retained.

Bommasani R. Lee T. Tsipras D. Soylu D. Yasunaga M. Zhang Y. Narayanan D. Wu Y.-Kumar A. et al. Liang, P. Holistic evaluation of language models, 2022. URL https://arxiv.org/abs/2211.09110. Verified scholarly preprint source for llm_evaluation; routed to Frameworks & Infrastructure (model evaluation); Security & Adversarial Considerations (model capability assessment); AGEINT Python Code Library. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: llm_evaluation. Source tier: scholarly_preprint. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for llm_evaluation materially changes. Verification method: direct_arxiv_record_review. Claim scope: Supports bounded AGEINT discussion of llm_evaluation and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that llm_evaluation claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_liang_2022_helm retained.

Andrew Zaldivar Mahima Pushkarna and Oddur Kjartansson. Data cards: Purposeful and transparent dataset documentation for responsible ai, 2022. URL https://arxiv.org/abs/2204.01075. ACM FAccT paper introducing Data Cards as structured, purposeful, human-centered summaries of dataset facts needed by stakeholders across a dataset lifecycle for responsible AI development. Checked as of 2026-06-09. Citation role: curriculum_anchor. Source lane: dataset_documentation. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: Data Cards paper, ACM record, arXiv record, dataset-documentation practice, or scholarly consensus materially changes. Verification method: direct_scholarly_page_review. Claim scope: Data Cards for purposeful, stakeholder-centered dataset documentation across origins, collection, annotation, intended use, evaluation context, lifecycle changes, and responsible AI review. Stakeholder role: data steward, dataset creator, model owner, assurance reviewer, instructor, learner, and affected-user representative. Assurance use: dataset card review, stakeholder-specific documentation checklist, dataset lifecycle governance, and model/data release evidence. Rights dimension: dataset transparency, stakeholder comprehension, fairness review, accountable reuse, and lifecycle documentation. Direct arXiv source URL verified live 2026-06-09 with title, authors, abstract, and ACM FAccT 2022 metadata matching the cited Data Cards paper.

Christopher W. Karvetski; David R. Mandel. Coherence of probability judgments from uncertain evidence: Does ach help?, 2020. URL https://www.cambridge.org/core/journals/judgment-and-decision-making/article/coherence-of-probability-judgments-from-uncertain-evidence-does-ach-help/9ED40E4658EE77914D2C7A265154B59A. Open Cambridge article testing whether ACH improves coherence of probabilistic judgments from uncertain evidence. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: sat_evaluation_evidence. Source tier: scholarly_peer_reviewed_open. Refresh cadence: annual. Refresh trigger: Publisher metadata, correction, or retraction status changes. Verification method: publisher_open_article_review. Claim scope: Supports bounded claims that ACH should be treated as a diagnostic aid whose probabilistic coherence gains are disputed and task-dependent. Stakeholder role: curriculum designer; forecasting instructor; analytic standards trainer. Assurance use: Anchors manuscript language that separates ACH transparency from accuracy or coherence proof. Rights dimension: open scholarly article; cite source and avoid extended quotation. Cambridge Core article page verified live 2026-06-15 for title, authors, journal record, and accessible article metadata.

David R. Mandel and Philip E. Tetlock. Correcting judgment correctives in national security intelligence, 2018. URL https://pmc.ncbi.nlm.nih.gov/articles/PMC6309046/. Peer-reviewed Frontiers in Psychology analysis (NIH PMC) on correcting judgment in national security intelligence, identifying neglect of noise and unipolar treatment of bipolar bias in IC debiasing. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: education_assessment. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: Updated peer-reviewed work on analytic debiasing, SAT validation, noise-versus-bias evidence, or replacement of the PMC landing record. Verification method: direct_scholarly_page_review. Claim scope: bias correction in national security intelligence, empirical limits of structured analytic techniques, unsystematic noise, and bipolar bias correction. Assurance use: analytic-bias review checklist, noise-versus-bias diagnostic, recalibration evidence, and SAT-validation critique. Direct source URL verified live (HTTP 200, on-topic NIH PMC peer-reviewed article) for AGEINT curriculum use.

John Wilcox; David R. Mandel. Critical review of the analysis of competing hypotheses technique: Lessons for the intelligence community, 2024. URL https://doi.org/10.1080/02684527.2024.2304934. Peer-reviewed critical review of ACH used to frame ACH as a diagnostic and review aid with contested efficacy claims. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: sat_evaluation_evidence. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: Publisher metadata, DOI record, correction, or retraction status changes. Verification method: crossref_doi_metadata_review. Claim scope: Supports bounded ACH caveats and lessons for intelligence practice, not claims that AGEINT validates ACH replacement or automation. Stakeholder role: analytic standards trainer; curriculum designer; evaluation lead. Assurance use: Strengthens SAT chapter language that separates hypothesis bookkeeping, diagnosticity review, and accuracy evidence. Rights dimension: copyrighted scholarly article; cite DOI metadata and summarize sparingly. Crossref DOI metadata verified live 2026-06-15 for title, authors, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.

Andrew Zaldivar Parker Barnes Lucy Vasserman Ben Hutchinson Elena Spitzer Inioluwa Deborah Raji Margaret Mitchell, Simone Wu and Timnit Gebru. Model cards for model reporting, 2019. URL https://arxiv.org/abs/1810.03993. Scholarly source for documenting intended use, evaluation procedures, benchmarked performance, limitations, and model-release context. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: model_card_reporting. Source tier: scholarly. Refresh cadence: annual. Refresh trigger: model reporting practice, model-card schema, or scholarly consensus changes. Verification method: direct_scholarly_page_review. Claim scope: model documentation cards, intended-use statements, evaluation caveats, and release notes. Stakeholder role: model steward, assurance reviewer, instructor, learner, and affected user. Assurance use: model card review and model-release evidence packet. Rights dimension: transparency, fairness, informed use, contestability, and accountable deployment. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Stephen Marrin. Improving intelligence analysis: Bridging the gap between scholarship and practice, 2012. URL https://doi.org/10.4324/9780203810200. Routledge scholarly book on linking intelligence-analysis scholarship and practice, used for tradecraft pedagogy and evidence-uptake framing. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: analytic_method_pedagogy. Source tier: scholarly_book_metadata. Refresh cadence: annual. Refresh trigger: Publisher metadata, DOI record, edition, or access status changes. Verification method: crossref_doi_metadata_review. Claim scope: Supports bounded claims about bridging intelligence scholarship, analytic practice, and training without treating scholarship uptake as a finished solution. Stakeholder role: curriculum designer; intelligence-studies instructor; methods reviewer. Assurance use: Connects SAT integration to a broader scholarship-practice gap rather than technique cataloging alone. Rights dimension: copyrighted scholarly book metadata only; cite and summarize sparingly. Crossref DOI metadata verified live 2026-06-15 for title, author, publisher, and year; DOI URL retained as stable scholarly source.

Michael J. Mazarr. Mastering the gray zone (usawc press, 2015), 2015. URL https://press.armywarcollege.edu/monographs/428/. Verified scholarly book metadata source for gray_zone_competition_doctrine; routed to Gray Zone / Hybrid Warfare / Non-State Actor Intelligence / Irregular Warfare. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: gray_zone_competition_doctrine. Source tier: scholarly_book_metadata. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for gray_zone_competition_doctrine materially changes. Verification method: direct_publisher_or_catalog_record_review. Claim scope: Supports bounded AGEINT discussion of gray_zone_competition_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that gray_zone_competition_doctrine claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source

education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_mazarr_2015_gray_zone retained.

Loren McCarthy. Seeing the futures: Evaluating the application of structured analytic technique alternative futures analysis, 2024. URL https://nationalsecurityjournal.nz/seeing-the-futures-evaluating-the-application-of-structured-analytic-technique-alternative-futures-analysis/. National Security Journal article evaluating Alternative Futures Analysis as an imaginative-thinking SAT and emphasizing purpose-fit and facilitator context. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: warning_intelligence. Source tier: scholarly_peer_reviewed_open. Refresh cadence: annual. Refresh trigger: Journal page, DOI 10.36878/nsj20241103.08, PDF, correction, or access status changes. Verification method: journal_page_and_doi_record_review. Claim scope: Supports bounded claims about Alternative Futures Analysis as a scenario and indicator aid whose value depends on purpose-fit and application context. Stakeholder role: warning instructor; curriculum designer; methods reviewer. Assurance use: Improves AFA and warning lessons without claiming scenario exercises predict the future. Rights dimension: open journal page; cite source and avoid extended quotation. National Security Journal article page verified live 2026-06-15 for title, author, publication date, DOI, abstract, and PDF link.

W. J. McGuire. Resistance to persuasion conferred by active and passive prior refutation of the same and alternative counterarguments, 1961. URL https://doi.apa.org/doi/10.1037/h0048344. The founding inoculation-theory experiment, showing that pre-exposing people to weakened counterarguments (refutational pre-bunking) builds resistance to later persuasion better than passive supportive defenses - the medical-vaccination analogy that grounds modern prebunking research. Checked as of 2026-06-08. Citation role: curriculum_anchor. Source lane: cognitive_influence_security. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: source URL, DOI, edition/standard version, or claim scope materially changes. Verification method: direct_source_url_review. Claim scope: Provides the historical and mechanistic foundation for AGEINT's inoculation/prebunking claims (the modern van der Linden and Roozenbeek literature), establishing that refutational pre-exposure confers durable resistance to influence operations. Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.

Gerald M. McMahon. Analytic tradecraft standards in an age of ai, 2024. URL https://www.belfercenter.org/research-analysis/analytic-tradecraft-standards-age-ai. Belfer Center Intelligence Project report on how AI tools interact with analytic tradecraft standards, especially source distinction, alternatives, uncertainty, and analyst ownership. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: analytic_tradecraft_evidence. Source tier: public_domain_primary. Refresh cadence: annual. Refresh trigger: Belfer report URL, PDF, DOI or citation metadata, or public analytic-tradecraft AI guidance materially changes. Verification method: primary_browser_report_page_review. Claim scope: Supports bounded discussion of analytic tradecraft standards under AI assistance; does not represent official U.S. government policy or validate AGEINT performance. Stakeholder role: analyst, tradecraft reviewer, AI governance reviewer, instructor. Assurance use: ICD 203 and AI-tool review, analyst-ownership checklist design, and tradecraft standards caveats. Rights dimension: analytic objectivity, accountability, civil liberties, public confidence, and human responsibility. Direct Belfer report page and linked PDF were verified on 2026-06-15 after the attachment URL had moved; title, author, publication date, and report scope were visible.

Surmon-Bohr F. Oleszkiewicz S. & Alison L. J. Meissner, C. A. Developing an evidence-based perspective on interrogation: A review of the u.s. government's high-value detainee interrogation group research program, 2017. URL https://doi.apa.org/doi/10.1037/law0000136. A peer-reviewed synthesis of the HIG-funded research program summarizing scores of empirical studies showing that rapport-based, non-coercive interviewing reliably outperforms accusatorial or coercive methods for eliciting accurate information, establishing the evidence base for rights-respecting elicitation. Checked as of 2026-06-08. Citation role: curriculum_anchor. Source lane: counterintelligence_source_integrity. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: source URL, DOI, edition/standard version, or claim scope materially changes. Verification method: direct_source_url_review. Claim scope: Backs the AGEINT claim that effective, evidence-based elicitation is rapport-based and rights-respecting rather than coercive. Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.

Siw Waffenschmidt Ana Patricia Ayala David Moher Matthew J. Page Jonathan B. Koffel Melissa L. Rethlefsen, Shona Kirtley and the PRISMA-S Group. Prisma-s: An extension to the prisma statement for reporting literature searches in systematic reviews, 2021. URL https://systematicreviewsjournal.biomedcentral.com/articles/10.1186/s13643-020-01542-z. Systematic Reviews article introducing the PRISMA-S extension, a 16-item checklist for transparent, reproducible reporting of search methods in evidence syntheses. Checked as of 2026-06-10. Citation role: curriculum_anchor. Source lane: source_construction_reporting. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: PRISMA-S guideline, PRISMA statement, systematic-review reporting practice, or journal record materially changes. Verification method: direct_scholarly_page_review. Claim scope: PRISMA-S reporting guideline for documenting literature searches, search strategies, information sources, limits, records, and reproducibility details. Stakeholder role: curriculum maintainer, assurance reviewer, instructor, learner, and source-refresh reviewer. Assurance use: source-construction reporting protocol, search-surface documentation, inclusion and exclusion evidence, deduplication notes, and refreshable citation workflow. Rights dimension: supports transparent source selection, reproducible search records, auditability, and limits on unverified discovery-source reuse. Direct journal landing page verified live 2026-06-10 with title, authors, publication date, journal metadata, and abstract describing the 16-item PRISMA-S checklist.

Dmitry I. Mikhailov. Optimizing national security strategies through llm-driven artificial intelligence integration, 2023. URL https://arxiv.org/abs/2305.13927. arXiv preprint on LLM-driven AI integration in national-security strategy, encoded with a narrow claim scope because it is useful as a strategic-policy framing source rather than as empirical validation. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: ai_enabled_analysis_boundary. Source tier: scholarly_preprint. Refresh cadence: semiannual. Refresh trigger: arXiv version, related DOI, national-security AI literature, or claim scope materially changes. Verification method: direct_arxiv_page_review. Claim scope: Provides discovery-grounded context for LLM-driven national-security strategy claims while requiring AGEINT prose to keep strategic claims bounded and evidence-bounded. Stakeholder role: policy analyst, AI governance reviewer, instructor. Assurance use: strategic-AI claim calibration and cautionary national-security AI planning context. Rights dimension: human oversight, strategic accountability, institutional due care, and non-escalatory educational framing. Direct arXiv source URL verified on 2026-06-15 with title, author, abstract, DOI metadata, and version history visible on the primary page.

Rad Miksa. Assessment tabling: An integrated structured analytic technique for improved intelligence analysis and reasoning visualisation, 2024. URL https://doi.org/10.1080/02684527.2024.2370129. Peer-reviewed article proposing assessment tabling as an integrated SAT and reasoning-visualization approach. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: analytic_method_pedagogy. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: Publisher metadata, DOI record, correction, or retraction status changes. Verification method: crossref_doi_metadata_review. Claim scope: Supports bounded claims about reasoning visualization as an analytic artifact design pattern, not empirical proof of accuracy improvement. Stakeholder role: methods instructor; visualization reviewer; curriculum designer. Assurance use: Feeds figure-caption and classroom-artifact language about visible reasoning without calling the visual a score. Rights dimension: copyrighted scholarly article; cite DOI metadata and summarize sparingly. Crossref DOI metadata verified live 2026-06-15 for title, author, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.

MITRE. Mitre atlas, 2026a. URL https://atlas.mitre.org/. MITRE ATLAS is a living knowledge base for adversarial threats to AI-enabled systems, useful for defensive red-team mapping and control coverage. Checked as of 2026-06-11. Citation role: curriculum_anchor. Source lane: ai_red_team_assurance. Source tier: research_standard. Refresh cadence: quarterly. Refresh trigger: MITRE ATLAS tactic, technique, mitigation, case-study, or matrix-version changes. Verification method: direct_standards_page_review. Claim scope: Adversarial Threat Landscape for Artificial-Intelligence Systems tactics, techniques, mitigations, and case-study vocabulary for defensive AI security analysis. Stakeholder role: AI

security analyst, red-team reviewer, incident responder, instructor, and learner. Assurance use: adversarial-AI threat taxonomy, defensive red-team mapping, AI control coverage, and incident-response exercise scoping. Rights dimension: security, accountable defensive testing, risk communication, incident readiness, and harm prevention. Direct MITRE ATLAS source URL verified live 2026-06-11; page identifies ATLAS as a globally accessible living knowledge base of adversary tactics and techniques against AI systems.

MITRE. Mitre att&ck enterprise matrix, 2026b. URL https://attack.mitre.org/matrices/enterprise/. Threat-informed enterprise matrix for defensive TTP mapping, coverage analysis, detection engineering, and analytic normalization. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: cyber_threat_intelligence. Source tier: research_standard. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

MITRE. Mitre att&ck for ics matrix, 2026c. URL https://attack.mitre.org/matrices/ics/. Threat-informed defensive matrix for ICS tactics and techniques, used for coverage mapping. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: ics_ot_defense. Source tier: research_standard. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

MITRE. D3fend matrix, 2026d. URL https://d3fend.mitre.org/. MITRE D3FEND knowledge base of cybersecurity countermeasure techniques and relationships to offensive/adversary techniques; used to ground defensive-control mapping without operationalizing attacks. Checked as of 2026-06-06. Citation role: curriculum_anchor. Source lane: assurance_evaluation_evidence. Source tier: research_standard. Refresh cadence: quarterly. Refresh trigger: D3FEND matrix, countermeasure taxonomy, ATT&CK relationship model, ontology release, or defensive-control mapping changes. Verification method: direct_official_page_review. Claim scope: defensive cybersecurity countermeasure taxonomy, relationships between defensive techniques and adversary techniques, and evidence-backed control selection. Stakeholder role: cyber defense analyst, control assessor, red-team debriefer, instructor, and learner. Assurance use: defensive-control crosswalk, countermeasure-evidence checklist, ATT&CK-to-D3FEND debrief, and assurance remediation backlog. Rights dimension: security, defensive proportionality, accountability, resilience, and harm prevention. Direct source URL verified live (HTTP 200, official MITRE D3FEND page with on-topic title and description metadata) for AGEINT curriculum use.

Center for Cryptologic History. National Security Agency. Nsa center for cryptologic history: Historical publications, Various years. URL https://www.nsa.gov/History/Cryptologic-History/Historical-Publications/. Verified official primary source for sigint_history; routed to SIGINT history; NSA organizational development; cryptologic heritage; ELINT/TELINT history. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: sigint_history. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for sigint_history materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of sigint_history and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that sigint_history claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_nsa_center_cryptologic_history_publications retained.

Cybersecurity National Security Agency, Infrastructure Security Agency, and Federal Bureau of Investigation. Contextualizing deepfake threats to organizations, 2023. URL https://media.defense.gov/2023/Sep/12/2003298925/-1/-1/0/CSI_DEEPFAKE_THREATS.PDF. Joint Cybersecurity Information Sheet on contextualizing deepfake threats, routed as official defensive guidance for provenance and synthetic-media risk review. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: synthetic_media_provenance. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: NSA/CISA/FBI deepfake guidance, PDF URL, or official synthetic-media threat framing materially changes. Verification method: direct_official_pdf_review. Claim scope: Supports defensive awareness and contextualization of deepfake threats; excludes impersonation guidance, targeting, evasion, and manipulation playbooks. Stakeholder role: cyber defender, cognitive-security reviewer, instructor, communications reviewer. Assurance use: deepfake-threat defensive control review, provenance triage, and public-sector awareness caveats. Rights dimension: identity protection, trust, privacy, safety, and defensive awareness. Direct defense.gov PDF source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

United Nations. Global digital compact, 2024. URL https://www.un.org/digital-emerging-technologies/global-digital-compact. United Nations Global Digital Compact page and adopted compact context for inclusive, rights-based digital cooperation and global AI governance. Checked as of 2026-05-24. Citation role: curriculum_anchor. Source lane: accessibility_digital_inclusion. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: UN Global Digital Compact implementation, adopted text, digital cooperation portal, AI governance, or digital-inclusion update. Verification method: direct_official_page_review. Claim scope: global digital cooperation, digital divides, human rights online, safe and secure digital future, and AI governance cooperation. Stakeholder role: rights reviewer, inclusion lead, instructor, learner, and public-interest steward. Assurance use: digital-inclusion and AI-governance crosswalk, human-rights review, public participation note, and inclusion evidence. Rights dimension: human rights, digital inclusion, accessibility, online safety, public participation, equality, and international cooperation. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Financial Crimes Enforcement Network. Fincen alerts, advisories, notices, bulletins, and fact sheets, 2026a. URL https://www.fincen.gov/resources/advisoriesbulletinsfact-sheets. Official FININT source for AML/CFT advisories, typology awareness, sanctions-evasion warnings, red flags, and compliance-oriented monitoring. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: financial_economic_security. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Financial Crimes Enforcement Network. Beneficial ownership information reporting, 2026b. URL https://www.fincen.gov/boi. Official FinCEN source for beneficial-ownership reporting, entity transparency, exemptions, and compliance-oriented analysis. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: financial_economic_security. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Financial Crimes Enforcement Network. Fincen sar narrative guidance package (2003/2006), FinCEN. URL https://www.fincen.gov/resources/statutes-regulations/guidance/sar-narrative-guidance-package. Verified official primary source for finint_sar_reporting; routed to Financial Intelligence (FININT). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: finint_sar_reporting. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for finint_sar_reporting materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of finint_sar_reporting and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that finint_sar_reporting claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review,

privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_fincen_sar_narrative_guidance retained.

Elaine Barker (NIST). Nist sp 800-57 part 1 rev. 5: Recommendation for key management, part 1: General, 2020. URL https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final. NIST's general guidance on cryptographic key management, covering key types, cryptoperiods, and lifecycle governance across the full key life. Checked as of 2026-06-08. Citation role: curriculum_anchor. Source lane: cyber_threat_intelligence. Source tier: technical_standard. Refresh cadence: annual. Refresh trigger: source URL, DOI, edition/standard version, or claim scope materially changes. Verification method: direct_source_url_review. Claim scope: Anchors the key-management / crypto-lifecycle governance discussion tying the cipher, signature, and hash standards into an operational regime. Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.

ASD ACSC NSA, CISA and partners. Principles for the secure integration of artificial intelligence in operational technology, 2025. URL https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4347041/nsa-cisa-and-others-release-guidance-on-integrating-ai-in-operational-technology/. Joint government guidance for AI governance, assurance, safety, and security in OT environments. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: ics_ot_defense. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

FBI et al. NSA, CISA. Prc state-sponsored cyber actor living off the land to evade detection (aa23-144a), 2023. URL https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a. Verified official primary source for apt_threat_intelligence; routed to Advanced Persistent Threats; Cyber Intelligence Fundamentals; ICS/OT Security. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: apt_threat_intelligence. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for apt_threat_intelligence materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of apt_threat_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that apt_threat_intelligence claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_cisa_aa23_144a_volt_typhoon_lotl retained.

Stanier I. Milne R. Shawyer A. & Walsh D. Nunan, J. Eliciting human intelligence: police source handlers' perceptions and experiences of rapport during covert human intelligence sources (chis) interactions, 2020. URL https://www.tandfonline.com/doi/full/10.1080/13218719.2020.1734978. A peer-reviewed study of UK police source handlers' lived perceptions of rapport during interactions with covert human intelligence sources, grounding how rapport functions in real source-handler tradecraft and the governance of HUMINT/CHIS relationships. Checked as of 2026-06-08. Citation role: curriculum_anchor. Source lane: counterintelligence_source_integrity. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: source URL, DOI, edition/standard version, or claim scope materially changes. Verification method: direct_source_url_review. Claim scope: Backs the AGEINT treatment of source-handler rapport and CHIS governance in operational HUMINT. Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.

OECD.AI Policy Observatory. Ai and work, 2026a. URL https://oecd.ai/en/dashboards/policy-areas/PA8. Official OECD.AI source for AI, work, labour-market transitions, skills, productivity, workplace governance, and policy responses. Checked as of 2026-06-06. Citation role: curriculum_anchor. Source lane: workforce_governance. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: OECD AI work theme, labour indicator, report, or policy-dashboard update. Verification method: direct_official_page_review. Claim scope: workforce transition, skills, productivity, workplace governance, and responsible adoption. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use; URL refreshed 2026-06-06 after liveness check.

OECD.AI Policy Observatory. Ai in the public sector, 2026b. URL https://oecd.ai/en/dashboards/policy-areas/PA12. Official OECD.AI source for public-sector AI adoption, governance, public value, accountability, and government service transformation. Checked as of 2026-06-06. Citation role: curriculum_anchor. Source lane: public_sector_agentic_ai. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: OECD public-sector theme, country practice, policy guidance, or measurement update. Verification method: direct_official_page_review. Claim scope: public-sector AI adoption, accountability, service design, and institutional capacity. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use; URL refreshed 2026-06-06 after liveness check.

OECD. Recommendation of the council on public procurement, 2015. URL https://legalinstruments.oecd.org/api/print?ids=320&lang=en. OECD public procurement legal instrument for transparency, integrity, access, risk management, accountability, evaluation, and supplier participation. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: procurement_vendor_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: OECD legal instrument revision, public procurement toolkit update, or procurement policy change. Verification method: direct_official_pdf_review. Claim scope: public procurement oversight, vendor-risk review, transparency, evaluation, and accountability. Stakeholder role: public buyer, vendor, contract manager, auditor, and affected public. Assurance use: vendor oversight gate, procurement evidence register, and contract-review checklist. Rights dimension: public accountability, fairness, transparency, and anti-corruption safeguards. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

OECD. Recommendation of the council on open government, 2017. URL https://legalinstruments.oecd.org/api/print?ids=359&lang=en. OECD open government legal instrument for transparency, integrity, accountability, stakeholder participation, civic space, and public-sector disclosure. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: public_sector_transparency. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: OECD open government legal instrument, public governance guidance, or civic-space update changes. Verification method: direct_official_pdf_review. Claim scope: public-sector transparency, accountable disclosure, stakeholder participation, and open-government review. Stakeholder role: public official, civic reviewer, instructor, affected community, and learner. Assurance use: public transparency statement and stakeholder-review evidence. Rights dimension: access to information, participation, accountability, and democratic governance. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

OECD. Oecd ai principles, 2024. URL https://oecd.ai/en/ai-principles. Official OECD principles for human-centered values, robustness, transparency, accountability, and inclusive AI growth. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: ai_ethics_data_governance. Source tier: international_standard. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

OECD. The agentic ai landscape and its conceptual foundations, 2026a. URL https://www.oecd.org/en/publications/the-agentic-ai-landscape-and-its-conceptual-foundations_396cf758-en.html. Official OECD conceptual foundation for agentic AI. Checked as of 2026-05-21. Citation role: source_quality_anchor. Source lane: source_quality_spine. Source tier: source_quality_anchor. Refresh cadence: semiannual. Refresh trigger: source version, legal status, standard revision, or official guidance changes. Verification method: direct_source_url_review. Claim scope: baseline source-quality guardrail for generated AGEINT curriculum claims. Stakeholder role: curriculum maintainer, instructor, reviewer, and learner.

Assurance use: source-quality triangulation and claim-boundary review. Rights dimension: source transparency, accountability, and evidence traceability. Directly verified official OECD source URL.

OECD. Artificial intelligence in education, 2026b. URL https://www.oecd.org/en/topics/sub-issues/artificial-intelligence-in-education.html. Official OECD topic page for AI in education, learning systems, assessment, teacher support, and education policy. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: education_assessment. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: OECD topic update, education report, indicator, or policy brief changes. Verification method: direct_official_page_review. Claim scope: education policy, assessment modernization, teacher support, and learner equity. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

OECD. Disinformation and misinformation, 2026c. URL https://www.oecd.org/en/topics/disinformation-and-misinformation.html. Official OECD policy source for information integrity, governance responses, public trust, and democratic resilience. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: cognitive_influence_security. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

International Society of Automation. Isa/iec 62443 series of standards, 2026. URL https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards. Official ISA overview of industrial automation and control security standards. Checked as of 2026-05-21. Citation role: source_quality_anchor. Source lane: source_quality_spine. Source tier: source_quality_anchor. Refresh cadence: semiannual. Refresh trigger: source version, legal status, standard revision, or official guidance changes. Verification method: direct_source_url_review. Claim scope: baseline source-quality guardrail for generated AGEINT curriculum claims. Stakeholder role: curriculum maintainer, instructor, reviewer, and learner. Assurance use: source-quality triangulation and claim-boundary review. Rights dimension: source transparency, accountability, and evidence traceability. Directly verified official ISA source URL.

Government of Canada. Ai strategy for the federal public service 2025-2027: Priority areas, 2025. URL https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/gc-ai-strategy-priority-areas.html. Government of Canada AI Strategy priority-area page for public-service AI adoption, governance, people, public value, and responsible implementation. Checked as of 2026-05-24. Citation role: curriculum_anchor. Source lane: workforce_governance. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: Canada AI Strategy 2025-2027 priority, implementation, workforce, governance, or public-service AI adoption changes. Verification method: direct_official_page_review. Claim scope: federal public-service AI strategy, governance priorities, talent, responsible adoption, public value, and implementation planning. Stakeholder role: public-sector AI leader, workforce planner, instructor, service steward, and learner. Assurance use: public-sector AI strategy crosswalk, workforce-readiness map, governance maturity review, and implementation evidence. Rights dimension: public value, accountable service delivery, workforce capability, inclusion, transparency, and trust. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Treasury Board of Canada Secretariat. Canada launches first register of ai uses in federal government, 2025. URL https://www.canada.ca/en/treasury-board-secretariat/news/2025/11/canada-launches-first-register-of-ai-uses-in-federal-government.html. Official announcement of Canada's federal AI register, used as a transparency anchor for AI use-case inventories and public-facing disclosure. Checked as of 2026-05-24. Citation role: curriculum_anchor. Source lane: public_sector_transparency. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: Canada AI register launch, register schema, public inventory, disclosure requirement, or federal AI-use publication changes. Verification method: direct_official_page_review. Claim scope: public AI register, government AI use disclosure, use-case inventory, public transparency, and refresh accountability. Stakeholder role: public official, transparency reviewer, records officer, instructor, and learner. Assurance use: public AI-use inventory review, disclosure checklist, register refresh, and transparency evidence. Rights dimension: public transparency, accountability, accessible notice, public trust, privacy, and service-user awareness. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Treasury Board of Canada Secretariat. Guide on the use of agentic artificial intelligence, 2026a. URL https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/guide-use-agentic-artificial-antelligence.html. Government of Canada guide for accountable public-sector use of agentic AI, including governance, risk, transparency, testing, monitoring, and human oversight considerations. Checked as of 2026-05-24. Citation role: curriculum_anchor. Source lane: public_sector_agentic_ai. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: Canada agentic-AI guide, public-sector AI policy, autonomy control, transparency, or monitoring guidance changes. Verification method: direct_official_page_review. Claim scope: agentic AI governance, bounded autonomy, human approval, monitoring, recoverability, and public-sector accountable deployment. Stakeholder role: public-sector AI steward, service owner, instructor, learner, and oversight reviewer. Assurance use: bounded-autonomy run card, recoverability review, approval threshold, monitoring evidence, and public-sector service assurance. Rights dimension: public trust, accountability, transparency, privacy, accessibility, human review, and service fairness. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Treasury Board of Canada Secretariat. Algorithmic impact assessment tool, 2026b. URL https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html. Government of Canada Algorithmic Impact Assessment tool for structured impact-level scoring, mitigation planning, and accountable review of automated decision systems. Checked as of 2026-05-24. Citation role: curriculum_anchor. Source lane: rights_impact_privacy. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: Algorithmic Impact Assessment tool, directive, scoring, mitigation, or government automated-decision policy changes. Verification method: direct_official_page_review. Claim scope: algorithmic impact assessment, risk level, mitigation evidence, accountability, and rights-impact review. Stakeholder role: AI program owner, privacy reviewer, rights-impact assessor, instructor, and learner. Assurance use: algorithmic impact worksheet, rights-risk triage, mitigation evidence, and review threshold. Rights dimension: privacy, equality, procedural fairness, redress, transparency, accessibility, and affected-group review. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

U.S. Department of Defense. Irregular warfare annex to the national defense strategy - summary (dod, 2020), 2020. URL https://media.defense.gov/2020/Oct/02/2002510472/-1/-1/0/Irregular-Warfare-Annex-to-the-National-Defense-Strategy-Summary.PDF. Verified official primary source for irregular_warfare_strategy; routed to Gray Zone / Hybrid Warfare / Non-State Actor Intelligence / Irregular Warfare. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: irregular_warfare_strategy. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for irregular_warfare_strategy materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of irregular_warfare_strategy and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that irregular_warfare_strategy claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_dod_iw_annex_2020 retained.

Council of Europe. Modernised convention for the protection of individuals with regard to the processing of personal data, 2018. URL https://www.coe.int/en/web/data-protection/convention108/modernised. Official Council of Europe source for Convention 108+ privacy, data-protection principles, transborder flows, and supervisory cooperation. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane:

human_rights_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: treaty status, ratification, explanatory report, or committee guidance changes. Verification method: direct_official_page_review. Claim scope: privacy governance, data-processing rights, oversight, and cross-border safeguards. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Council of Europe. Framework convention on artificial intelligence, 2024. URL https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence. Official treaty anchor for human rights, democracy, rule-of-law, risk management, accountability, and public-sector AI governance. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: legal_oversight. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

NATO Cooperative Cyber Defence Centre of Excellence. New ccdcoe research reconceptualises cognitive warfare, 2026. URL https://ccdcoe.org/news/2026/new-ccdcoe-research-reconceptualises-cognitive-warfare/. CCDCOE 2026 research reconceptualising cognitive warfare as a contest over the structures of interpretation and decision-making rather than information content; introduces systemic invariants and cognitive decoherence. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: human_rights_governance. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: CCDCOE cognitive warfare research, systemic-invariants model, cognitive-decoherence framing, or NATO CoE cognitive-security publication changes. Verification method: direct_official_page_review. Claim scope: cognitive warfare as a contest over interpretive structures, systemic invariants (trust, identity, epistemic standards), and cognitive decoherence in sociotechnical systems. Direct source URL verified live (HTTP 200, on-topic CCDCOE cognitive-warfare research) for AGEINT curriculum use.

NATO Strategic Communications Centre of Excellence. Nato stratcom coe strategic communications hybrid threats toolkit (2021), 2021. URL https://stratcomcoe.org/publications/download/Strategic-Communications-Hybrid-Threats-Toolkit.pdf. Verified official primary source for hybrid_warfare_stratcom; routed to Gray Zone / Hybrid Warfare / Non-State Actor Intelligence / Irregular Warfare; Active Measures and Disinformation. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: hybrid_warfare_stratcom. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for hybrid_warfare_stratcom materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of hybrid_warfare_stratcom and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that hybrid_warfare_stratcom claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_nato_stratcom_hybrid_threats_toolkit retained.

Egmont Group of Financial Intelligence Units. Egmont group principles for information exchange between fius (april 2023), 2023. URL https://egmontgroup.org/wp-content/uploads/2022/07/2.-Principles-Information-Exchange-With-Glossary_April2023.pdf. Verified official primary source for finint_international_cooperation; routed to Financial Intelligence (FININT). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: finint_international_cooperation. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for finint_international_cooperation materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of finint_international_cooperation and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that finint_international_cooperation claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_egmont_group_fiu_principles retained.

Office of Foreign Assets Control. A framework for ofac compliance commitments, 2019. URL https://ofac.treasury.gov/media/16331/download?inline. Official OFAC compliance framework for management commitment, risk assessment, internal controls, testing, auditing, and training. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: financial_economic_security. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Office of Foreign Assets Control. Sanctions programs and country information, 2026. URL https://ofac.treasury.gov/sanctions-programs-and-country-information. Official OFAC sanctions-program library for understanding legal program structure, list maintenance, and compliance-oriented economic statecraft. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: financial_economic_security. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Forum of Incident Response and Security Teams. Traffic light protocol (tlp) - first standards definitions and usage guidance, version 2.0, FIRST. URL https://www.first.org/tlp/. Verified official primary source for threat_intel_sharing_standards; routed to Threat Intelligence Sharing for Critical Infrastructure; Cyber Intelligence Fundamentals. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: threat_intel_sharing_standards. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for threat_intel_sharing_standards materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of threat_intel_sharing_standards and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that threat_intel_sharing_standards claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_first_tlp_v2 retained.

Bureau of Industry and Security. Export enforcement, 2026. URL https://www.bis.gov/enforcement. Official export-control enforcement source for compliance, screening, red flags, voluntary disclosures, and national-security protection of sensitive items. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: financial_economic_security. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Federal Bureau of Investigation. Counterintelligence and espionage, 2026. URL https://www.fbi.gov/investigate/counterintelligence. FBI public counterintelligence page describing defensive goals and protection of IC secrets, critical assets, and sensitive information. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: counterintelligence_program_governance. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: FBI page content, URL, or public counterintelligence mission framing materially changes. Verification method: browser_fetch_official_html_review. Claim scope: public counterintelligence mission and defensive source-integrity context. Stakeholder role: CI

reviewer, analyst, instructor. Assurance use: supports defensive CI/source-integrity framing without investigation procedure or surveillance guidance. Rights dimension: public education page used for defensive awareness and source-protection framing. Direct URL verified on 2026-06-14 through browser search/open because fbi.gov returned 403 to plain curl; fetched content matched the Counterintelligence and Espionage page.

U.S. Department of Justice. Fact sheet: New rule on the accessibility of web content and mobile apps provided by state and local governments, 2024. URL https://www.ada.gov/resources/2024-03-08-web-rule/. DOJ ADA Title II fact sheet for state and local government web and mobile app accessibility obligations, WCAG technical standard use, contractors, and compliance timing. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: accessibility_digital_inclusion. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: ADA Title II rule, Federal Register update, compliance date, or DOJ guidance changes. Verification method: direct_official_page_review. Claim scope: public-sector accessibility obligations, contractor oversight, and digital-service compliance review. Stakeholder role: public entity, contractor, learner, disabled service user, and compliance reviewer. Assurance use: public-sector accessibility gate and vendor deliverable review. Rights dimension: disability rights, equal access, and public-service inclusion. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Joint Chiefs of Staff. Jp 3-13, information operations (2012), 2012. URL https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/12102012_io1.pdf. Verified official primary source for information_operations_doctrine; routed to Information Warfare and Cognitive Security; PSYOP and MISO Doctrine. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: information_operations_doctrine. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for information_operations_doctrine materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of information_operations_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that information_operations_doctrine claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_dod_jp3_13_information_operations retained.

Joint Chiefs of Staff. Jp 2-0, joint intelligence (2013), 2013. URL https://irp.fas.org/doddir/dod/jp2_0.pdf. Verified official primary source for imint_joint_intelligence_doctrine; routed to Imagery Intelligence (IMINT); Counterintelligence. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: imint_joint_intelligence_doctrine. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for imint_joint_intelligence_doctrine materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of imint_joint_intelligence_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that imint_joint_intelligence_doctrine claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_dod_jp2_0_joint_intelligence retained.

Joint Chiefs of Staff. Jp 3-05, special operations (2014), 2014a. URL https://edocs.nps.edu/2014/July/jp3_05.pdf. Verified official primary source for special_operations_doctrine; routed to Gray Zone / Hybrid Warfare / Non-State Actor Intelligence / Irregular Warfare; Counterintelligence. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: special_operations_doctrine. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for special_operations_doctrine materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of special_operations_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that special_operations_doctrine claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_dod_jp3_05_special_operations retained.

Joint Chiefs of Staff. Jp 3-13.2, military information support operations (2014), 2014b. URL https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Joint_Staff/Military_Information_Support_Operations.pdf. Verified official primary source for psyop_miso_doctrine; routed to PSYOP and MISO Doctrine; Information Warfare and Cognitive Security. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: psyop_miso_doctrine. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for psyop_miso_doctrine materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of psyop_miso_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that psyop_miso_doctrine claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_dod_jp3_13_2_miso retained.

Joint Chiefs of Staff. Jp 2-0: Joint intelligence, 2026. URL https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/2-0-Intelligence-Series/. Official joint-doctrine landing page for the keystone publication on joint intelligence principles, products, services, and assessments. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: collection_management. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology (NIST). Fips 197: Advanced encryption standard (aes), 2001. URL https://csrc.nist.gov/pubs/fips/197/final. The U.S. federal standard specifying the AES block cipher, the canonical symmetric algorithm providing data confidentiality. Checked as of 2026-06-08. Citation role: curriculum_anchor. Source lane: cyber_threat_intelligence. Source tier: technical_standard. Refresh cadence: annual. Refresh trigger: source URL, DOI, edition/standard version, or claim scope materially changes. Verification method: direct_source_url_review. Claim scope: Anchors the symmetric-encryption / confidentiality element of the SIGINT chapter's crypto-assurance discussion. Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.

National Institute of Standards and Technology (NIST). Fips 180-4: Secure hash standard (shs), 2015. URL https://csrc.nist.gov/pubs/fips/180-4/upd1/final. The U.S. federal standard specifying the SHA family of cryptographic hash functions used to produce fixed-length digests for data-integrity verification. Checked as of 2026-06-08. Citation role: curriculum_anchor. Source lane: cyber_threat_intelligence. Source tier: technical_standard. Refresh cadence: annual. Refresh trigger: source URL, DOI, edition/standard version, or claim scope materially changes. Verification method: direct_source_url_review. Claim scope: Anchors the integrity / hashing layer of the SIGINT chapter's crypto-assurance discussion. Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.

National Institute of Standards and Technology (NIST). Fips 186-5: Digital signature standard (dss), 2023. URL https://csrc.nist.gov/pubs/fips/186-5/final. The U.S. federal standard specifying approved digital-signature algorithms (e.g., ECDSA, EdDSA, RSA) used to authenticate signatories and detect unauthorized data modification. Checked as of 2026-06-08. Citation role: curriculum_anchor. Source lane: cyber_threat_intelligence. Source tier: technical_standard. Refresh cadence: annual. Refresh trigger: source URL, DOI, edition/standard version, or claim scope materially changes. Verification method: direct_source_url_review. Claim scope: Anchors the digital-signature / authentication / provenance element of the crypto-assurance figure. Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.

National Institute of Standards and Technology. Guide to test, training, and exercise programs for it plans and capabilities, 2006. URL https://csrc.nist.gov/pubs/sp/800/84/final. Official methodology for designing, conducting, and evaluating test, training, and exercise programs. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: ics_ot_defense. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Information security continuous monitoring, nist sp 800-137, 2011a. URL https://csrc.nist.gov/pubs/sp/800/137/final. Official continuous-monitoring guidance for metrics, status awareness, ongoing authorization, and governance feedback loops. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: cyber_threat_intelligence. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Managing information security risk, nist sp 800-39, 2011b. URL https://csrc.nist.gov/pubs/sp/800/39/final. Official enterprise-risk source for mission, organization, and system tiers, risk framing, assessment, response, and monitoring. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: legal_oversight. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Guide for conducting risk assessments, nist sp 800-30 rev. 1, 2012. URL https://csrc.nist.gov/pubs/sp/800/30/r1/final. Official risk-assessment method for threat, vulnerability, impact, likelihood, uncertainty, and residual-risk reasoning. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: legal_oversight. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Guide to cyber threat information sharing, nist sp 800-150, 2016. URL https://csrc.nist.gov/pubs/sp/800/150/final. Official guidance for establishing threat-information sharing goals, communities, distribution rules, and defensive use of indicators and TTPs. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: cyber_threat_intelligence. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Framework for cyber-physical systems: Volume 1, overview, 2017. URL https://www.nist.gov/publications/framework-cyber-physical-systems-volume-1-overview. Official NIST cyber-physical systems framework for functions, timing, trustworthiness, interoperability, and safety-aware architecture. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: ics_ot_defense. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Protecting information and system integrity in industrial control system environments, nist sp 1800-10, 2018a. URL https://csrc.nist.gov/pubs/sp/1800/10/final. Official NCCoE practice guide for manufacturing-sector ICS integrity, monitoring, architecture, and defensive lab validation. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: ics_ot_defense. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Risk management framework for information systems and organizations, nist sp 800-37 rev. 2, 2018b. URL https://csrc.nist.gov/pubs/sp/800/37/r2/final. Official RMF lifecycle source for preparation, categorization, control selection, implementation, assessment, authorization, and monitoring. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: legal_oversight. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Security and privacy controls for information systems and organizations, nist sp 800-53 rev. 5, 2020a. URL https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final. Official security and privacy control catalog for control baselines, assessment language, privacy controls, and inherited-control reasoning. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: legal_oversight. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Zero trust architecture, nist sp 800-207, 2020b. URL https://csrc.nist.gov/pubs/sp/800/207/final. Official zero-trust architecture guidance for identity-centric authorization, continuous evaluation, least privilege, and policy enforcement. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: agentic_ai_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Enhanced security requirements for protecting controlled unclassified information, nist sp 800-172, 2021. URL https://csrc.nist.gov/pubs/sp/800/172/final. Official enhanced security requirements for high-value CUI, source handling analogies, system integrity, and advanced persistent threat resistance. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: counterintelligence_source_integrity. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Towards a standard for identifying and managing bias in artificial intelligence, 2022a. URL https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf. Official NIST source for AI bias concepts, socio-technical framing, measurement limits, and governance-oriented mitigation. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: ai_ethics_data_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Engineering trustworthy secure systems, nist sp 800-160 vol. 1 rev. 1, 2022b. URL https://csrc.nist.gov/pubs/sp/800/160/v1/r1/final. Systems-security engineering foundation for trustworthy systems in contested operational environments and related training programs. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: ics_ot_defense. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Cybersecurity supply chain risk management practices, nist sp 800-161 rev. 1, 2022c. URL https://csrc.nist.gov/pubs/sp/800/161/r1/upd1/final. Official supply-chain risk-management guidance for identifying, assessing, and mitigating product, service, vendor, and process risks. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: cyber_threat_intelligence. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Secure software development framework, nist sp 800-218, 2022d. URL https://csrc.nist.gov/pubs/sp/800/218/final. Official secure development framework for agent tooling, connectors, and software supply chains. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: agentic_ai_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Artificial intelligence risk management framework (ai rmf 1.0), 2023. URL https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf. Official NIST.AI.100-1 risk-management framework. Checked as of 2026-05-21. Citation role: source_quality_anchor. Source lane: source_quality_spine. Source tier: source_quality_anchor. Refresh cadence: semiannual. Refresh trigger: source version, legal status, standard revision, or official guidance changes. Verification method: direct_source_url_review. Claim scope: baseline source-quality guardrail for generated AGEINT curriculum claims. Stakeholder role: curriculum maintainer, instructor, reviewer, and learner. Assurance use: source-quality triangulation and claim-boundary review. Rights dimension: source transparency, accountability, and evidence traceability. Directly verified official NIST source URL.

National Institute of Standards and Technology. Adversarial machine learning: A taxonomy and terminology of attacks and mitigations, 2024a. URL https://csrc.nist.gov/pubs/ai/100/2/e2023/final. Official adversarial-ML taxonomy for defensive AI threat modeling, mitigation vocabulary, evaluation limits, and safe red-team framing. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: agentic_ai_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Reducing risks posed by synthetic content: An overview of technical approaches to digital content transparency, 2024b. URL https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-4.pdf. NIST AI 100-4 report on reducing risks posed by synthetic content through digital content transparency, provenance, labeling, watermarking, detection, testing, auditing, and maintenance approaches. Checked as of 2026-06-11. Citation role: curriculum_anchor. Source lane: model_data_provenance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: NIST AI 100-4 revision, synthetic-content transparency standard, provenance technology, watermarking guidance, or digital-content policy materially changes. Verification method: direct_official_pdf_review. Claim scope: Synthetic-content provenance, watermarking, labeling, detection, testing, auditing, maintenance, disclosure, and digital content transparency for generated media and influence-risk review. Stakeholder role: provenance reviewer, model-card steward, synthetic-media evaluator, instructor, learner, and affected-person representative. Rights dimension: transparency, provenance, disclosure, privacy, child safety, non-consensual intimate imagery prevention, and accountable synthetic-media governance. Direct NIST AI 100-4 PDF and publication landing page verified live 2026-06-11; report covers provenance, labeling, watermarking, detection, testing, auditing, and maintenance.

National Institute of Standards and Technology. A plan for global engagement on ai standards, 2024c. URL https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-5.pdf. NIST AI 100-5 plan for global engagement on AI standards, used to ground standards coordination and cross-jurisdiction AI-governance discussions without claiming a single universal compliance regime. Checked as of 2026-06-06. Citation role: curriculum_anchor. Source lane: ai_conformity_compliance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: NIST global AI standards plan, standards-development priorities, international AI standards coordination, or conformity-assessment guidance changes. Verification method: direct_official_pdf_review. Claim scope: global AI standards engagement, standards-development coordination, AI governance interoperability, and conformity-assessment planning. Stakeholder role: standards lead, compliance reviewer, procurement assessor, instructor, and learner. Rights dimension: accountability, interoperability, standards participation, transparency, and cross-border governance consistency. Direct source URL verified live (HTTP 200 PDF, title metadata and first pages on-topic) for AGEINT curriculum use.

National Institute of Standards and Technology. Artificial intelligence risk management framework: Generative ai profile, 2024d. URL https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf. Official NIST AI 600-1 generative AI profile. Checked as of 2026-05-21. Citation role: source_quality_anchor. Source lane: source_quality_spine. Source tier: source_quality_anchor. Refresh cadence: semiannual. Refresh trigger: source version, legal status, standard revision, or official guidance changes. Verification method: direct_source_url_review. Claim scope: baseline source-quality guardrail for generated AGEINT curriculum claims. Stakeholder role: curriculum maintainer, instructor, reviewer, and learner. Assurance use: source-quality triangulation and claim-boundary review. Rights dimension: source transparency, accountability, and evidence traceability. Directly verified official NIST source URL.

National Institute of Standards and Technology. Artificial intelligence risk management framework: Generative artificial intelligence profile, 2024e. URL https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf. NIST AI 600-1 profile for generative AI risk management, risk framing, evaluation actions, misuse considerations, and AI RMF alignment. Checked as of 2026-06-11. Citation role: curriculum_anchor. Source lane: assurance_evaluation_evidence. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: NIST AI 600-1 revision, AI RMF profile update, generative-AI risk guidance, or evaluation action changes. Verification method: direct_official_pdf_review. Claim scope: Generative-AI risk profile, AI RMF implementation actions, evaluation controls, misuse-risk review, and trustworthiness evidence mapping. Stakeholder role: AI governance lead, assurance reviewer, instructor, system steward, procurement assessor, and learner. Assurance use: AI risk profile crosswalk, generative-AI evaluation evidence, misuse-risk review, and source-backed trustworthiness caveats. Rights dimension: trustworthy AI, safety, security, privacy, fairness, transparency, accountability, and documented evaluation limits. Direct NIST AI 600-1 PDF and NIST publication landing page verified live 2026-06-11 for GenAI Profile scope and AI RMF alignment.

National Institute of Standards and Technology. The nist cybersecurity framework (csf) 2.0, 2024f. URL https://www.nist.gov/publications/nist-cybersecurity-framework-csf-20. Official cybersecurity-risk governance framework that adds the Govern function and supplies a common language for AI, OT, and enterprise risk. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: ics_ot_defense. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Fips 203: Ml-kem post-quantum key-encapsulation standard, 2024a. URL https://csrc.nist.gov/pubs/fips/203/final. Verified official primary source for cryptography_standards; routed to Cryptography standards; post-quantum SIGINT resilience; communications security modernization. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: cryptography_standards. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for cryptography_standards materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of cryptography_standards and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that cryptography_standards claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_nist_fips_203_ml_kem retained.

National Institute of Standards and Technology. Fips 204: Ml-dsa post-quantum digital signature standard, 2024b. URL https://csrc.nist.gov/pubs/fips/204/final. Verified official primary source for cryptography_standards; routed to Cryptography standards; post-quantum digital signatures; authentication in collection systems. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: cryptography_standards. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for cryptography_standards materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of cryptography_standards and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that cryptography_standards claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_nist_fips_204_ml_dsa retained.

National Institute of Standards and Technology. Fips 205: Slh-dsa post-quantum hash-based signature standard, 2024c. URL https://csrc.nist.gov/pubs/fips/205/final. Verified official primary source for cryptography_standards; routed to Cryptography standards; post-quantum signature diversity; long-term data integrity. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: cryptography_standards. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for cryptography_standards materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of cryptography_standards and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that cryptography_standards claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_nist_fips_205_slh_dsa retained.

National Institute of Standards and Technology. Mapping relationships between documentary standards, regulations, frameworks, and guidelines, nist ir 8477, 2024. URL https://csrc.nist.gov/pubs/ir/8477/final. Official mapping-method source for comparing controls, regulations, frameworks, and guidance without collapsing their separate purposes. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: legal_oversight. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Nist ir 8547: Transition to post-quantum cryptography standards, 2024. URL https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf. Verified official draft source for cryptographic_standards; routed to Cryptographic Methods appendix; Security & Adversarial Considerations. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: cryptographic_standards. Source tier: official_draft. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for cryptographic_standards materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of cryptographic_standards and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that cryptographic_standards claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_nist_pqc_migration_ir8547 retained.

National Institute of Standards and Technology. Secure software development practices for generative ai and dual-use foundation models, 2024a. URL https://csrc.nist.gov/pubs/sp/800/218/a/final. NIST SSDF Community Profile for AI model development, AI systems using models, AI system acquisition, and secure lifecycle practices. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: secure_release_change_control. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: NIST SSDF, SP 800-218A, generative-AI profile, or AI secure-development practice changes. Verification method: direct_official_page_review. Claim scope: release gates, secure lifecycle controls, AI model acquisition, and change-control evidence. Stakeholder role: system steward, security reviewer, vendor assessor, instructor, and learner. Assurance use: release and change-control gate with secure-development evidence. Rights dimension: security, resilience, due care, accountability, and harm prevention. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Guide to operational technology security, nist sp 800-82 rev. 3, 2024b. URL https://csrc.nist.gov/pubs/sp/800/82/r3/final. Official NIST operational technology security guidance. Checked as of 2026-05-21. Citation role: source_quality_anchor. Source lane: source_quality_spine. Source tier: source_quality_anchor. Refresh cadence: semiannual. Refresh trigger: source version, legal status, standard revision, or official guidance changes. Verification method: direct_source_url_review. Claim scope: baseline source-quality guardrail for generated AGEINT curriculum claims. Stakeholder role: curriculum maintainer, instructor, reviewer, and learner. Assurance use: source-quality triangulation and claim-boundary review. Rights dimension: source transparency, accountability, and evidence traceability. Directly verified official NIST source URL.

National Institute of Standards and Technology. Assessing risks and impacts of ai (aria): Pilot evaluation report, 2025a. URL https://www.nist.gov/publications/assessing-risks-and-impacts-ai-aria-pilot-evaluation-report. NIST ARIA pilot report describing evaluation scenarios, model testing, red teaming, field testing, dialogue annotation, tester questionnaires, and measurement trees. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: assurance_evaluation_evidence. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: ARIA

evaluation program, pilot report, scenario design, or AI measurement guidance changes. Verification method: direct_official_page_review. Claim scope: assurance evaluation evidence, scenario design, red-team testing, field testing, and measurement trees. Stakeholder role: assurance lead, evaluator, instructor, learner, and affected user. Assurance use: agent evaluation protocol and adversarial assurance evidence. Rights dimension: validity, reliability, safety, fairness, user impact, and accountable testing. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Digital identity guidelines, nist sp 800-63-4, 2025b. URL https://csrc.nist.gov/pubs/sp/800/63/4/final. Official digital-identity guidance for authentication, federation, identity proofing, and agent/tool authorization analogies. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: agentic_ai_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Incident response recommendations and considerations, nist sp 800-61 rev. 3, 2025c. URL https://csrc.nist.gov/pubs/sp/800/61/r3/final. Official incident-response profile for preparation, detection, response, recovery, and continuous improvement under CSF 2.0. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: cyber_threat_intelligence. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Incident response recommendations and considerations for cybersecurity risk management: A csf 2.0 community profile, 2025d. URL https://csrc.nist.gov/pubs/sp/800/61/r3/final. NIST SP 800-61 Rev. 3 source for integrating incident response with risk management, preparation, detection, response, and recovery. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: agent_incident_response. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: NIST SP 800-61 revision, CSF 2.0 community profile update, or incident-response terminology changes. Verification method: direct_official_page_review. Claim scope: agent incident tabletop design, incident lifecycle, recovery evidence, and post-incident review. Stakeholder role: incident commander, system steward, instructor, learner, and risk owner. Assurance use: agent incident response drill and escalation evidence. Rights dimension: resilience, accountability, due care, and harm minimization. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Accelerating the adoption of software and artificial intelligence agent identity and authorization, 2026a. URL https://csrc.nist.gov/pubs/other/2026/02/05/accelerating-the-adoption-of-software-and-ai-agent/ipd. NIST concept paper for applying identity and authorization standards to software and AI agents. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: agentic_ai_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Practices for automated benchmark evaluations of language models and ai agent systems, nist ai 800-2 initial public draft, 2026b. URL https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.800-2.ipd.pdf. NIST AI 800-2 initial public draft provides voluntary practices for automated benchmark evaluations of language models and AI agent systems. Checked as of 2026-06-11. Citation role: curriculum_anchor. Source lane: assurance_evaluation_evidence. Source tier: official_draft. Refresh cadence: quarterly. Refresh trigger: NIST AI 800-2 draft revision, final publication, benchmark evaluation practice update, public comment resolution, or agent-system evaluation guidance changes. Verification method: direct_official_pdf_review. Claim scope: Initial public draft practices for automated benchmark evaluations of language models and AI agent systems, including defining evaluation context, conducting benchmark evaluation, and communicating results. Stakeholder role: AI evaluator, procurement assessor, assurance reviewer, instructor, system steward, and learner. Assurance use: automated benchmark evaluation protocol, agent benchmark documentation, validity and reproducibility review, and evaluation-report caveats. Rights dimension: validity, reliability, reproducibility, transparency, accountability, procurement review, and documented evaluation limits. Direct NIST AI 800-2 PDF and NIST announcement verified live 2026-06-11; draft status retained explicitly for AGEINT curriculum use.

National Institute of Standards and Technology. Ai agent standards initiative, 2026c. URL https://www.nist.gov/artificial-intelligence/ai-agent-standards-initiative. Official NIST initiative for trusted, interoperable, and secure AI-agent standards, protocols, identity, and evaluation research. Checked as of 2026-06-11. Citation role: curriculum_anchor. Source lane: agent_interoperability_standards. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: NIST AI-agent standards initiative, RFI, guidance, technical convening, protocol, identity, or evaluation deliverable changes. Verification method: direct_official_page_review. Claim scope: AI-agent interoperability, secure delegation, agent identity, standards gaps, protocol coordination, and evaluation research for autonomous digital actors. Stakeholder role: standards steward, agent architect, assurance reviewer, procurement assessor, instructor, and learner. Assurance use: agent standards crosswalk, secure delegation review, identity evidence, interoperability claims, and evaluation-scope caveats. Rights dimension: secure delegated action, accountable non-human identity, interoperability, least-privilege user control, and auditable agent behavior. Direct NIST source URL verified live 2026-06-11; page identifies the AI Agent Standards Initiative as focused on trusted, interoperable, and secure agentic AI.

National Institute of Standards and Technology. Nist ai resource center, 2026d. URL https://airc.nist.gov/. NIST AI Resource Center source for AI RMF operationalization, playbook resources, crosswalks, profiles, and testing, evaluation, verification, and validation support. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: ai_red_team_assurance. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: AI RMF revision, playbook revision, AIRC technical reports, or TEVV resources change. Verification method: direct_official_page_review. Claim scope: AI RMF operationalization, TEVV evidence, crosswalks, profiles, and assurance planning. Stakeholder role: assurance lead, instructor, compliance reviewer, and learner. Assurance use: TEVV evidence plan and AI RMF crosswalk. Rights dimension: trustworthy AI, accountability, safety, and rights-preserving evaluation. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Concept note: Ai rmf profile on trustworthy ai in critical infrastructure, 2026e. URL https://www.nist.gov/programs-projects/concept-note-ai-rmf-profile-trustworthy-ai-critical-infrastructure. NIST concept note for a critical-infrastructure AI RMF profile covering AI-enabled IT, OT, and industrial-control environments. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: assurance_evaluation_evidence. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: NIST AI RMF critical-infrastructure profile concept, draft, final profile, or public-comment update. Verification method: direct_official_page_review. Claim scope: critical-infrastructure AI trustworthiness, AI RMF profiling, infrastructure risk review, and sector assurance evidence. Stakeholder role: critical-infrastructure steward, OT defender, assurance reviewer, instructor, and learner. Assurance use: critical-infrastructure AI RMF profile crosswalk and tabletop assurance review. Rights dimension: safety, resilience, reliability, security, public service continuity, and accountable infrastructure governance. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Nist ai rmf playbook, 2026f. URL https://airc.nist.gov/airmf-resources/playbook/. Official AI RMF playbook for translating Govern, Map, Measure, and Manage functions into curriculum controls and review prompts. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: ai_ethics_data_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Ai research: Security and resilience, 2026g. URL https://www.nist.gov/artificial-intelligence/ai-research-security-and-resilience. NIST AI security and resilience research hub for secure-and-resilient AI trustworthiness, adversarial machine learning taxonomy, and mitigation work. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: ai_red_team_assurance. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: NIST AI security report, adversarial machine learning taxonomy, or AI RMF security update changes. Verification method: direct_official_page_review. Claim scope: AI red-team assurance, adversarial ML terminology, mitigation taxonomy, and resilience evidence. Stakeholder role: red-team reviewer, assurance lead, instructor, and learner. Assurance use: adversarial assurance cycle and mitigation evidence. Rights dimension: security, reliability, harm prevention, and accountable AI testing. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Nist big data interoperability framework, 2026h. URL https://www.nist.gov/publications/nist-big-data-interoperability-framework-volume-1-definitions. Official NIST program source for big-data interoperability, reference architecture, data interfaces, vocabulary, and technology roadmap. Checked as of 2026-06-06. Citation role: curriculum_anchor. Source lane: model_data_provenance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: NIST big-data framework volume, version, roadmap, or program update. Verification method: direct_official_page_review. Claim scope: data interoperability, architecture vocabulary, data lifecycle, and provenance-aware systems. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use; URL refreshed 2026-06-06 after liveness check.

National Institute of Standards and Technology. Dioptra, 2026i. URL https://pages.nist.gov/dioptra/. NIST Dioptra test platform for evaluating AI system risks, adversarial robustness, and measurement workflows in controlled settings. Checked as of 2026-05-24. Citation role: curriculum_anchor. Source lane: ai_red_team_assurance. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: NIST Dioptra release, documentation, testbed capability, AI measurement, or adversarial-evaluation update. Verification method: direct_official_page_review. Claim scope: AI testbed evaluation, adversarial testing, red-team assurance, reproducible measurement, and risk assessment workflow. Stakeholder role: assurance evaluator, red-team reviewer, instructor, system steward, and learner. Assurance use: AI red-team testbed evidence, reproducible evaluation run, measurement packet, and assurance artifact. Rights dimension: trustworthy AI, safety, security, validity, reliability, transparency, and accountable testing. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Institute of Standards and Technology. Oscal - open security controls assessment language, 2026j. URL https://pages.nist.gov/OSCAL/. NIST Open Security Controls Assessment Language project, used to ground machine-readable control catalogs, assessment evidence, and compliance traceability. Checked as of 2026-06-06. Citation role: curriculum_anchor. Source lane: records_retention_auditability. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: OSCAL model version, NIST control catalog, assessment result schema, component definition, or compliance automation guidance changes. Verification method: direct_official_page_review. Claim scope: machine-readable security controls, assessment plans/results, system security plans, component definitions, and compliance evidence exchange. Stakeholder role: control assessor, compliance engineer, audit-trail steward, instructor, and learner. Assurance use: machine-readable control-evidence package, assessment-result review, audit-trail crosswalk, and compliance automation readiness check. Rights dimension: accountability, auditability, transparency, security, privacy, and due-process traceability. Direct source URL verified live (HTTP 200, official NIST OSCAL page) for AGEINT curriculum use.

National Institute of Standards and Technology. Nist privacy framework, 2026k. URL https://www.nist.gov/privacy-framework. Official privacy risk-management framework for identifying and managing privacy risk, data governance, workforce roles, and enterprise controls. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: privacy_ip_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

United States Department of State. Open source intelligence strategy, 2024. URL https://2021-2025.state.gov/open-source-intelligence-strategy/. Official strategy source for lawful OSINT governance, discovery, validation, and dissemination. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: osint_geoint. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Department of the Army. Atp 2-33.4: Intelligence analysis, 2020. URL https://rdl.train.army.mil/catalog-ws/view/100.ATSC/F4DDBAD5-3131-4C2A-9E00-CCACC087E984-1408655126204/ATP2_33x4wc1.pdf. Official Army analytic doctrine for intelligence-analysis process, structured analytic techniques, analytic design, and cognitive discipline. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: analytic_tradecraft. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

U.S. Department of the Army. Fm 2-22.3 human intelligence collector operations, 2006. URL https://www.marines.mil/Portals/1/Publications/FM%202-22.3%20%20Human%20Intelligence%20Collector%20Operations_1.pdf. Verified official primary source for humint_doctrine; routed to HUMINT collection discipline; source operations; interrogation ethics and doctrine. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: humint_doctrine. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for humint_doctrine materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of humint_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that humint_doctrine claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_army_fm_2_22_3_humint retained.

Office of the Director of National Intelligence. Icd 302: Document and media exploitation, 2007. URL https://www.dni.gov/files/documents/ICD/ICD-302.pdf. Verified official primary source for humint_doctrine; routed to HUMINT collection; document and media analyzeation; all-source integration. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: humint_doctrine. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for humint_doctrine materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of humint_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that humint_doctrine claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_odni_icd_302_domex retained.

Office of the Director of National Intelligence. Intelligence community directive 207: National intelligence council, 2008. URL https://www.dni.gov/files/documents/ICD/ICD-207.pdf. ODNI directive describing the National Intelligence Council and national intelligence production responsibilities. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: national_intelligence_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: ODNI directive version, source URL, or policy text materially changes. Verification method: browser_fetch_official_pdf_review. Claim scope: IC governance and national-intelligence production context. Stakeholder role: analyst, instructor,

governance reviewer. Assurance use: anchors national intelligence council references to public ODNI policy text. Rights dimension: public directive used for governance education and source routing. Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 207.

Office of the Director of National Intelligence. Icd 304: Human intelligence, 2008. URL https://www.odni.gov/files/documents/ICD/ICD-304.pdf. Verified official primary source for humint_doctrine; routed to HUMINT governance; IC collection management; CI integration. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: humint_doctrine. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for humint_doctrine materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of humint_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that humint_doctrine claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_odni_icd_304_humint retained.

Office of the Director of National Intelligence. Intelligence community directive 209: Tearline production and dissemination, 2012. URL https://www.dni.gov/files/documents/ICD/ICD-209-Tearline-Production-and-Dissemination.pdf. ODNI directive for tearlines and broader dissemination while protecting sources and methods. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: tearlines_and_release_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: ODNI directive version, source URL, or policy text materially changes. Verification method: browser_fetch_official_pdf_review. Claim scope: tearline and release-governance support for public-facing evidence boundaries. Stakeholder role: analyst, disclosure reviewer, instructor. Assurance use: anchors safe discussion of sanitized outputs without teaching live release decisions. Rights dimension: public directive used for governance education, not disclosure authorization. Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 209.

Office of the Director of National Intelligence. Intelligence community directive 205: Analytic outreach, 2013a. URL https://www.dni.gov/files/documents/ICD/ICD-205-Analytic-Outreach.pdf. ODNI directive for analytic outreach, outside expertise, risk management, and citation of outreach insights. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: analytic_outreach_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: ODNI directive version, source URL, or policy text materially changes. Verification method: browser_fetch_official_pdf_review. Claim scope: analytic-outreach governance support for expert engagement and risk controls. Stakeholder role: analyst, outreach lead, reviewer. Assurance use: supports source-pack routing for external expertise while preserving CI, privacy, and citation boundaries. Rights dimension: public directive used for governance education, not outreach tasking. Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF title and text matched ICD 205 Analytic Outreach.

Office of the Director of National Intelligence. Intelligence community directive 403: Foreign disclosure and release of classified national intelligence, 2013b. URL https://www.dni.gov/files/documents/ICD/ICD-403.pdf. ODNI directive for foreign disclosure and release governance, marking, records, and release authority. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: foreign_disclosure_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: ODNI directive version, source URL, or policy text materially changes. Verification method: browser_fetch_official_pdf_review. Claim scope: foreign-disclosure governance support for release-boundary and control-marking lessons. Stakeholder role: disclosure reviewer, analyst, instructor. Assurance use: supports evidence-bounded disclosure-boundary teaching and release-control caveats. Rights dimension: public directive used for governance education, not disclosure authorization. Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 403.

Office of the Director of National Intelligence. Intelligence community directive 710: Classification and control markings system, 2013c. URL https://www.dni.gov/files/documents/ICD/ICD-710.pdf. ODNI directive for classification and control markings, including release and foreign-disclosure marking relationships. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: classification_marking_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: ODNI directive version, source URL, or policy text materially changes. Verification method: browser_fetch_official_pdf_review. Claim scope: classification-marking context for caveat and dissemination-boundary lessons. Stakeholder role: marking reviewer, analyst, instructor. Assurance use: anchors marking references to public ODNI policy without handling classified material. Rights dimension: public directive used for governance education, not classification authority. Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 710.

Office of the Director of National Intelligence. Intelligence community directive 731: Supply chain risk management, 2013d. URL https://www.dni.gov/files/documents/ICD/ICD-731-Supply-Chain-Risk-Management.pdf. ODNI directive for IC supply-chain risk management across mission-critical products, materials, and services. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: supply_chain_risk_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: ODNI directive version, source URL, or policy text materially changes. Verification method: browser_fetch_official_pdf_review. Claim scope: supply-chain risk governance support for defensive procurement and assurance lessons. Stakeholder role: procurement reviewer, security analyst, instructor. Assurance use: supports supplier-risk and source-integrity language without evasion or exploitation guidance. Rights dimension: public directive used for governance education and defensive assurance. Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 731.

Office of the Director of National Intelligence. Intelligence community directive 750: Counterintelligence programs, 2013e. URL https://www.dni.gov/files/documents/ICD/ICD-750.pdf. ODNI directive establishing a baseline for counterintelligence programs across the IC. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: counterintelligence_program_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: ODNI directive version, source URL, or policy text materially changes. Verification method: browser_fetch_official_pdf_review. Claim scope: counterintelligence program governance support for source-integrity and defensive awareness. Stakeholder role: CI reviewer, analyst, instructor. Assurance use: supports defensive CI/source-integrity language without surveillance or handling playbooks. Rights dimension: public directive used for governance education and defensive source-integrity framing. Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 750.

Office of the Director of National Intelligence. Intelligence community directive 900: Integrated mission management, 2013f. URL https://www.dni.gov/files/documents/ICD/ICD-900-Integrated-Mission-Managemement.pdf. ODNI directive for integrated mission management and IC mission alignment. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: integrated_mission_management. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: ODNI directive version, source URL, or policy text materially changes. Verification method: browser_fetch_official_pdf_review. Claim scope: mission-management governance support for requirements-to-evidence substrate design. Stakeholder role: mission manager, analyst, governance reviewer. Assurance use: anchors mission-alignment language in public ODNI policy. Rights dimension: public directive used for governance education and source routing. Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 900.

Office of the Director of National Intelligence. Intelligence community directive 203: Analytic standards, 2015. URL https://www.intel.gov/assets/documents/Intelligence%20Community%20Directives/ICD_203.pdf. Official ODNI analytic tradecraft standards directive. Checked as of 2026-05-21. Citation role: source_quality_anchor. Source lane: source_quality_spine. Source tier: source_quality_anchor. Refresh cadence: semiannual. Refresh trigger: source version, legal status, standard revision, or official guidance changes. Verification method: direct_source_url_review. Claim scope: baseline source-quality guardrail for generated AGEINT curriculum claims. Stakeholder role: curriculum maintainer, instructor, reviewer,

and learner. Assurance use: source-quality triangulation and claim-boundary review. Rights dimension: source transparency, accountability, and evidence traceability. Directly verified official ODNI source URL.

Office of the Director of National Intelligence. Icd 310: Coordination of clandestine human source collection outside the us, 2016. URL https://www.dni.gov/files/documents/ICD/ICD-310-Coord-of-Clandestine-Human-and-Human-enabled-FI-and-CI-outside-the-US-2016-06-27.pdf. Verified official primary source for humint_doctrine; routed to HUMINT deconfliction; CI integration; overseas collection coordination. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: humint_doctrine. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for humint_doctrine materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of humint_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that humint_doctrine claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_odni_icd_310_clandestine_humint_outside_us retained.

Office of the Director of National Intelligence. Intelligence community directive 121: Managing the intelligence community information environment, 2017a. URL https://www.dni.gov/files/documents/ICD/ICD-121-Managing-the-IC-Information-Environment-2017-01-19.pdf. ODNI directive for the IC information environment, discovery, retrieval, sharing, and safeguarding. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: ic_information_environment_risk. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: ODNI directive version, source URL, or policy text materially changes. Verification method: browser_fetch_official_pdf_review. Claim scope: information environment support for modular discovery, retrieval, and safeguarding claims. Stakeholder role: system owner, analyst, reviewer. Assurance use: anchors substrate modularity in information-sharing and safeguarding governance. Rights dimension: public directive used for governance education, not classified system operation. Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 121.

Office of the Director of National Intelligence. Intelligence community directive 208: Maximizing the utility of analytic products, 2017b. URL https://www.dni.gov/files/documents/ICD/ICD-208-Maximizing-the-Utility-of-Analytic-Products-2017-01-09.pdf. ODNI directive for customer utility, analytic standards, tearlines, discoverability, and transparent products. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: analytic_product_dissemination. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: ODNI directive version, source URL, or policy text materially changes. Verification method: browser_fetch_official_pdf_review. Claim scope: analytic-product utility, discoverability, and dissemination-governance support. Stakeholder role: analyst, editor, dissemination reviewer. Assurance use: supports generated prose about product utility, reusable evidence packets, and customer-aware outputs. Rights dimension: public directive used for governance education, not release authorization. Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 208.

Office of the Director of National Intelligence. Intelligence community directive 211: Ic support to the cfius threat analysis process, 2022. URL https://www.dni.gov/files/documents/ICD/ICD-211-CFIUS-09-04-22-REDACTED.pdf. ODNI directive for intelligence support to CFIUS threat analysis, economic-security review, and covered transactions. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: economic_security_review. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: ODNI directive version, source URL, or policy text materially changes. Verification method: browser_fetch_official_pdf_review. Claim scope: economic-security and due-diligence governance support for threat-analysis framing. Stakeholder role: economic-security analyst, reviewer, instructor. Assurance use: supports safe CFIUS-context teaching without transaction targeting or proprietary data use. Rights dimension: public directive used for governance education and due-diligence framing. Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 211.

Office of the Director of National Intelligence. Odni commercially available information fact sheet (may 2024), 2024. URL https://www.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Fact-Sheet-May2024.pdf. Verified official primary source for osint_doctrine; routed to OSINT/PAI governance; CAI policy framework; privacy in collection. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: osint_doctrine. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for osint_doctrine materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of osint_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that osint_doctrine claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_odni_cai_fact_sheet_2024 retained.

Office of the Director of National Intelligence. Intelligence community directive 405: Intelligence diplomacy, 2024a. URL https://www.dni.gov/files/documents/ICD/ICD-405-Intelligence-Diplomacy.pdf. ODNI directive for intelligence diplomacy, synchronization, and foreign-policy support boundaries. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: intelligence_diplomacy_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: ODNI directive version, source URL, or policy text materially changes. Verification method: browser_fetch_official_pdf_review. Claim scope: governance context for intelligence diplomacy and partner-engagement boundaries. Stakeholder role: policy reviewer, analyst, instructor. Assurance use: keeps diplomacy references policy-bound and evidence-bounded. Rights dimension: public directive used for governance education, not diplomatic action guidance. Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 405.

Office of the Director of National Intelligence. Intelligence community directive 406: Ic engagement with non-state entities, 2024b. URL https://www.dni.gov/files/documents/ICD/ICD-406-IC-Engagement-with-Non-State-Entities.pdf. ODNI directive for non-state entity engagement, analytic outreach, privacy/civil-liberties, and no-tasking boundaries. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: non_state_engagement_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: ODNI directive version, source URL, or policy text materially changes. Verification method: browser_fetch_official_pdf_review. Claim scope: non-state engagement governance support for source, outreach, and no-tasking boundaries. Stakeholder role: outreach lead, analyst, reviewer. Assurance use: anchors public-source and expert-engagement rules without authorizing collection tasking. Rights dimension: public directive used for governance education and civil-liberties framing. Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 406.

Office of the Director of National Intelligence. Intelligence community directive 503: Intelligence community information environment risk management, 2024c. URL https://www.dni.gov/files/documents/ICD/ICD-503.pdf. ODNI directive for risk management in the IC information environment. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: ic_information_environment_risk. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: ODNI directive version, source URL, or policy text materially changes. Verification method: browser_fetch_official_pdf_review. Claim scope: information-environment risk governance support for secure, auditable intelligence systems. Stakeholder role: security reviewer, system owner, instructor. Assurance use: supports modular substrate controls around access, risk, and auditability. Rights dimension: public directive used for governance education, not classified-system design. Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF content matched ICD 503.

Office of the Director of National Intelligence. Intelligence community directive 504: Intelligence community data management, 2025a. URL https://www.dni.gov/files/documents/ICD/ICD-504.pdf. Official IC data-management directive for data governance, data stewardship, CDO authority, interoperability, and data lifecycle management. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: ai_ethics_data_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Office of the Director of National Intelligence. Intelligence community directive 505: Artificial intelligence, 2025b. URL https://www.dni.gov/files/documents/ICD/ICD-505-Artificial-Intelligence.pdf. Official IC AI governance directive covering CAIO roles, oversight, interoperability, civil-liberties review, training data, and impact assessment. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: ai_ethics_data_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Office of the Director of National Intelligence. Annual threat assessment of the u.s. intelligence community 2026, 2026a. URL https://www.dni.gov/files/ODNI/documents/assessments/ATA-2026-Unclassified-Report.pdf. ODNI unclassified annual threat assessment used as current public threat-context baseline, not as operational guidance. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: current_threat_baseline. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: new Annual Threat Assessment, source URL change, or report correction is released. Verification method: browser_fetch_official_pdf_review. Claim scope: public threat-context grounding and warning-topic baseline, not operational targeting or AGEINT benchmark evidence. Stakeholder role: analyst, instructor, policy reviewer. Assurance use: anchors public threat-context examples to an official unclassified IC baseline. Rights dimension: public unclassified report used for education and contextual analysis. Direct URL verified on 2026-06-14 through browser fetch because dni.gov returned 403 to plain curl; fetched PDF title and content matched the Annual Threat Assessment.

Office of the Director of National Intelligence. Authorized classification and control markings register, 2026b. URL https://www.dni.gov/files/documents/FOIA/Authorized%20Classification%20and%20Control%20Markings%20Register%20V1.2.pdf. Official CAPCO register for classification and control-marking vocabulary, abbreviations, portion markings, and dissemination syntax. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: governed_intelligence_cycle. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Office of the Director of National Intelligence. Intelligence community directive 204: National intelligence priorities framework, 2026c. URL https://www.dni.gov/files/documents/ICD/ICD_204_National_Intelligence_Priorities_Framework_U_FINAL-SIGNED.pdf. Official prioritization directive for translating national intelligence priorities into collection, analysis, risk management, and responsiveness evaluation. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: collection_management. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Office of the Director of National Intelligence. Intelligence community directive 206: Sourcing requirements for disseminated analytic products, 2026d. URL https://www.dni.gov/files/documents/ICD/ICD-206.pdf. Official sourcing directive for traceability, citations, source descriptors, and source summaries. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: analytic_tradecraft. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Office of the Director of National Intelligence. Objectivity and ic analytic standards, 2026e. URL https://www.intel.gov/mission/our-values/objectivity. Official ODNI explanation of analytic objectivity, ombuds, and tradecraft standards. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: analytic_tradecraft. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Office of the Director of National Intelligence. Icd 206: Sourcing requirements for disseminated analytic products (with ics 206-01 on pai/cai/osint), Current. URL https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives. Verified official primary source for osint_doctrine; routed to OSINT sourcing standards; analytic product integrity; IC information sourcing discipline. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: osint_doctrine. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for osint_doctrine materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of osint_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that osint_doctrine claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_odni_icd_206_sourcing_osint_pai retained.

Office of the Director of National Intelligence and Central Intelligence Agency. The int of first resort: The ic osint strategy 2024-2026, 2024. URL https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf. Official IC OSINT strategy for professionalizing OSINT, integrated collection management, open-source sharing, innovation, and tradecraft. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: osint_geoint. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Chairman of the Joint Chiefs of Staff. Jp 2-01: Joint and national intelligence support to military operations (2012), 2012. URL https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Joint_Staff/21-F-0090_Document_1.pdf. Verified official primary source for collection_management_doctrine; routed to All-source collection management; HUMINT/SIGINT/GEOINT integration; joint intelligence support. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: collection_management_doctrine. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for collection_management_doctrine materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of collection_management_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that collection_management_doctrine claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_jp_2_01_intelligence_support_2012 retained.

Chairman of the Joint Chiefs of Staff. Jp 2-03: Geospatial intelligence in joint operations (2017), 2017. URL https://irp.fas.org/doddir/dod/jp2_03.pdf. Verified official primary source for geoint_doctrine; routed to GEOINT doctrine; imagery intelligence in joint operations; NGA role; GEOINT organizations. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: geoint_doctrine. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for geoint_doctrine materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of geoint_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that geoint_doctrine claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_jp_2_03_geoint_joint_ops_2017 retained.

Executive Office of the President. M-25-21: Accelerating federal use of ai through innovation, governance, and public trust, 2025a. URL https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf. OMB memorandum for federal AI strategies, AI maturity, data traceability, continuous monitoring, governance, privacy, security, workforce, and public trust. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: risk_exception_governance. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: OMB federal AI governance memo, agency strategy requirement, traceability, or monitoring guidance changes. Verification method: direct_official_pdf_review. Claim scope: risk exception governance, AI maturity plans, data traceability, public trust, and oversight capacity. Stakeholder role: agency AI officer, risk owner, instructor, oversight reviewer, and learner. Assurance use: risk exception memo and agency AI governance crosswalk. Rights dimension: public trust, privacy, security, accessibility, transparency, and accountable governance. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Executive Office of the President. M-25-22: Driving efficient acquisition of artificial intelligence in government, 2025b. URL https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-22-Driving-Efficient-Acquisition-of-Artificial-Intelligence-in-Government.pdf. OMB memorandum for federal AI acquisition, product demonstrations, performance-based requirements, Quality Assurance Surveillance Plans, monitoring, and transparency requirements. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: procurement_performance_monitoring. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: OMB AI acquisition memo, QASP guidance, solicitation transparency, or monitoring requirement changes. Verification method: direct_official_pdf_review. Claim scope: AI procurement monitoring, vendor demonstrations, acquisition criteria, QASP evidence, and performance review. Stakeholder role: procurement official, vendor assessor, instructor, system steward, and learner. Assurance use: procurement oversight loop and vendor-performance monitoring packet. Rights dimension: transparent acquisition, vendor accountability, public value, interoperability, and due care. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Office of the United Nations High Commissioner for Human Rights. Digital space and human rights, 2026a. URL https://www.ohchr.org/en/digital-space-and-human-rights. Official OHCHR portal for human rights in digital space, including technology, privacy, civic space, equality, and remedy concerns. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: human_rights_governance. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: OHCHR thematic report, mandate, or digital-rights guidance updates. Verification method: direct_official_page_review. Claim scope: rights impact mapping, privacy, expression, civic space, remedy, and digital governance. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Office of the United Nations High Commissioner for Human Rights. The right to privacy in the digital age, 2026b. URL https://www.ohchr.org/en/privacy-in-the-digital-age. Official OHCHR privacy-in-the-digital-age page for surveillance, data protection, AI, remedy, and human-rights safeguards. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: human_rights_governance. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: UN report, resolution, special procedure, or digital privacy guidance changes. Verification method: direct_official_page_review. Claim scope: privacy rights, data protection, surveillance safeguards, and rights-based AI review. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Reconnaissance Office. Declassified nro programs and projects, 2026a. URL https://www.nro.gov/foia-home/foia-declassified-nro-programs-and-projects/. Official declassified satellite-reconnaissance program archive for CORONA, GAMBIT, POPPY, QUILL, and other historical technical-intelligence cases. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: historical_declassified_sources. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

National Reconnaissance Office. About nro history, 2026b. URL https://www.nro.gov/About-NRO/history/. NRO public history page describing the Center for the Study of National Reconnaissance and declassified history resources. Checked as of 2026-06-14. Citation role: curriculum_anchor. Source lane: declassified_reconnaissance_history. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: NRO history page content, URL, or declassification-resource structure materially changes. Verification method: browser_fetch_official_html_review. Claim scope: declassified reconnaissance history support for historical and GEOINT source-provenance lessons. Stakeholder role: historian, GEOINT analyst, instructor. Assurance use: anchors national reconnaissance history to official declassified-history resources. Rights dimension: public history page used for education and source-provenance review. Direct URL verified on 2026-06-14 through web search/open; official NRO page content matched the history and Center for the Study of National Reconnaissance description.

United States Copyright Office. Copyright and artificial intelligence, part 3: Generative ai training, 2025. URL https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-3-Generative-AI-Training-Report-Pre-Publication-Version.pdf. Official U.S. copyright policy source for generative-AI training, rights-holder impacts, transparency, licensing, and IP governance. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: privacy_ip_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

U.S. Government Accountability Office. Artificial intelligence: An accountability framework for federal agencies and other entities, 2021. URL https://www.gao.gov/products/gao-21-519sp. Official GAO accountability framework for AI governance, data, performance, monitoring, and accountability evidence. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: ai_conformity_compliance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: GAO supplement, agency guidance, or framework revision changes. Verification method: direct_official_page_review. Claim scope: AI accountability controls, data governance, performance monitoring, and audit evidence. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Senior Advisory Group Panel. Office of the Director of National Intelligence. Odni declassified report on commercially available information (2022), 2022. URL https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf. Verified official primary source for osint_doctrine; routed to OSINT/PAI doctrine; commercially available information; privacy and civil liberties in collection. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: osint_doctrine. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for osint_doctrine materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of osint_doctrine and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance,

manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that osint_doctrine claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_odni_cai_report_2022 retained.

& Phythian Mark. Omand, David. Principled spying - georgetown university press, 2018. URL https://press.georgetown.edu/Book/Principled-Spying. Verified scholarly book metadata source for ethics_of_intelligence; routed to Ethics of Intelligence and Cognitive Security; HUMINT ethics; surveillance ethics; oversight accountability. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: ethics_of_intelligence. Source tier: scholarly_book_metadata. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for ethics_of_intelligence materially changes. Verification method: direct_publisher_or_catalog_record_review. Claim scope: Supports bounded AGEINT discussion of ethics_of_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that ethics_of_intelligence claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_omand_phythian_2018_principled_spying retained.

David. Omand. Securing the state - google books, 2010. URL https://books.google.com/books/about/Securing_the_State.html?id=G9FmSQAACAAJ. Verified scholarly book metadata source for ethics_of_intelligence; routed to Ethics of Intelligence and Cognitive Security; legal and ethical constraints on secret intelligence; oversight principles. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: ethics_of_intelligence. Source tier: scholarly_book_metadata. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for ethics_of_intelligence materially changes. Verification method: direct_publisher_or_catalog_record_review. Claim scope: Supports bounded AGEINT discussion of ethics_of_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that ethics_of_intelligence claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_omand_2010_securing_the_state retained.

United Nations Office on Drugs and Crime. Unodc money laundering, proceeds of crime and the financing of terrorism, UNODC. URL https://www.unodc.org/unodc/en/money-laundering/index.html. Verified official primary source for finint_aml_cft_international; routed to Financial Intelligence (FININT). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: finint_aml_cft_international. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for finint_aml_cft_international materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of finint_aml_cft_international and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that finint_aml_cft_international claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_unodc_money_laundering_overview retained.

United States Senate Select Committee on Intelligence. Report on the u.s. intelligence community's prewar intelligence assessments on iraq, 2004. URL https://www.intelligence.senate.gov/sites/default/files/publications/108301.pdf. Official Senate report on prewar Iraq intelligence assessments used as postmortem context for assumptions, dissent, caveats, and source-confidence failures. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: intelligence_failure_postmortem. Source tier: official_report. Refresh cadence: biennial. Refresh trigger: Senate report URL, archival location, or official record status changes. Verification method: direct_official_pdf_review. Claim scope: Supports bounded postmortem claims about Iraq WMD assessment failures and the need for explicit assumptions, source quality, dissent, and caveats. Stakeholder role: curriculum designer; governance reviewer; analytic tradecraft instructor. Assurance use: Prevents failure lessons from implying that any single SAT would have prevented a complex institutional failure. Rights dimension: public-domain government report; cite official source. Official Senate Intelligence Committee PDF URL verified live 2026-06-15 with successful redirect to current Senate-hosted PDF asset.

National Commission on Terrorist Attacks Upon the United States. The 9/11 commission report, 2004. URL https://9-11commission.gov/report/911Report.pdf. Official commission report used for postmortem context on warning, information sharing, imagination, and reform pressures after September 11, 2001. Checked as of 2026-06-11. Citation role: curriculum_anchor. Source lane: intelligence_failure_postmortem. Source tier: official_report. Refresh cadence: biennial. Refresh trigger: Refresh if official commission site or report URL changes. Verification method: direct_pdf_download. Claim scope: Supports bounded claims about post-9/11 warning and reform context. Stakeholder role: curriculum designer; governance reviewer; analyst supervisor. Assurance use: Connects warning lessons to postmortem learning and reform without hindsight simplification. Rights dimension: public-domain government report; cite official source. Official commission PDF verified live 2026-06-11; use for postmortem and reform context, not as a one-size failure formula.

Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. Report to the president of the united states: The commission on the intelligence capabilities of the united states regarding weapons of mass destruction, 2005. URL https://policy.defense.gov/portals/11/Documents/hdasa/references/GPO-WMD.pdf. Official WMD Commission report used for Iraq WMD analytic-failure context, assumptions-versus-evidence boundaries, and reform pressure. Checked as of 2026-06-11. Citation role: curriculum_anchor. Source lane: intelligence_failure_postmortem. Source tier: official_report. Refresh cadence: biennial. Refresh trigger: Refresh if official hosted PDF or archival record changes. Verification method: direct_pdf_download. Claim scope: Supports bounded claims about Iraq WMD intelligence failure, assumptions, evidence gaps, and analytic reform. Stakeholder role: curriculum designer; governance reviewer; analytic tradecraft instructor. Assurance use: Shows why evidence boundaries, dissent, and assumption registers matter in high-consequence analysis. Rights dimension: public-domain government report; cite official source. Defense policy-hosted official report PDF verified live 2026-06-11; use for assumptions/evidence and analytic-failure context.

OASIS Open. Common security advisory framework version 2.0, 2022. URL https://docs.oasis-open.org/csaf/csaf/v2.0/os/csaf-v2.0-os.html. OASIS Common Security Advisory Framework Version 2.0 standard for machine-readable vulnerability and remediation advisories, used to ground audit-ready incident and procurement evidence. Checked as of 2026-06-12. Citation role: curriculum_anchor. Source lane: records_retention_auditability. Source tier: technical_standard. Refresh cadence: annual. Refresh trigger: CSAF version, errata, vulnerability-advisory schema, product-status vocabulary, remediation field, or OASIS standard status changes. Verification method: direct_standards_page_review. Claim scope: machine-readable security advisories, vulnerability disclosure structure, product status, remediation metadata, and advisory exchange governance. Stakeholder role: PSIRT lead, vulnerability coordinator, procurement reviewer, instructor, and learner. Assurance use: security-advisory evidence package, vulnerability-status table, remediation-record review, and supplier disclosure audit. Rights dimension: security transparency, accountable disclosure, remediation traceability, procurement accountability, and harm reduction. Direct canonical OASIS OS HTML source URL verified live (HTTP 200, CSAF Version 2.0 OASIS Standard page on-topic) for AGEINT curriculum use.

International Labour Organization. Global commission on the future of work, 2019. URL https://www.ilo.org/resource/news/global-commission-

future-work. Official ILO source for a human-centred future-of-work agenda, lifelong learning, labour guarantees, social protection, and decent work. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: workforce_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: ILO centenary initiative, commission follow-up, decent-work agenda, or policy update. Verification method: direct_official_page_review. Claim scope: human-centred labour governance, lifelong learning, worker protection, and social dialogue. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

International Labour Organization. Artificial intelligence, 2026a. URL https://www.ilo.org/topics-and-sectors/artificial-intelligence. Official ILO topic page for AI and work, digital transformation, occupational impact, skills, safety, and social dialogue. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: workforce_governance. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: ILO AI topic update, report, policy note, or labour-market evidence update. Verification method: direct_official_page_review. Claim scope: workforce impact, decent work, skills, social dialogue, and AI adoption governance. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

International Labour Organization and United Nations. Mind the ai divide: Shaping a global perspective on the future of work, 2024. URL https://www.ilo.org/publications/major-publications/mind-ai-divide-shaping-global-perspective-future-work. Official ILO/UN publication on uneven AI adoption, labour-market exposure, global equity, fairness, and social justice. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: workforce_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: ILO/UN report revision, follow-up data, or labour-market exposure model update. Verification method: direct_publication_page_review. Claim scope: workforce equity, adoption gaps, labour-market exposure, and global AI governance. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

North Atlantic Treaty Organization. Countering information threats, 2026b. URL https://www.nato.int/cps/en/natohq/topics_219728.htm. Official NATO counter-information-threat guidance. Checked as of 2026-05-21. Citation role: source_quality_anchor. Source lane: source_quality_spine. Source tier: source_quality_anchor. Refresh cadence: semiannual. Refresh trigger: source version, legal status, standard revision, or official guidance changes. Verification method: direct_source_url_review. Claim scope: baseline source-quality guardrail for generated AGEINT curriculum claims. Stakeholder role: curriculum maintainer, instructor, reviewer, and learner. Assurance use: source-quality triangulation and claim-boundary review. Rights dimension: source transparency, accountability, and evidence traceability. Directly verified official NATO source URL.

North Atlantic Treaty Organization. Countering hybrid threats, 2026c. URL https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats. Official NATO source for hybrid-threat resilience across cyber, information, economic, political, and military pressure. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: cognitive_influence_security. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

World Intellectual Property Organization. Artificial intelligence and intellectual property, 2026d. URL https://www.wipo.int/en/web/frontier-technologies/artificial-intelligence/index. Official WIPO source for AI and IP policy, training-data rights, copyright infrastructure, transparency, attribution, and member-state dialogue. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: privacy_ip_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

James Pamment and Victoria Smith. Attributing information influence operations (nato stratcom coe, 2022), 2022. URL https://stratcomcoe.org/publications/download/Nato-Attributing-Information-Influence-Operations-DIGITAL-v4.pdf. Verified official primary source for active_measures_attribution; routed to Active Measures and Disinformation; Counterintelligence; Information Warfare and Cognitive Security. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: active_measures_attribution. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for active_measures_attribution materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of active_measures_attribution and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that active_measures_attribution claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_nato_stratcom_attributing_iio retained.

Joseph C.; Cai Carrie J.; Morris Meredith Ringel; Liang Percy; Bernstein Michael S. Park, Joon Sung; O'Brien. Generative agents: Interactive simulacra of human behavior, 2023. URL https://arxiv.org/abs/2304.03442. Demonstrates a multi-agent sandbox of twenty-five LLM agents whose memory-stream, reflection, and planning architecture produces believable emergent social behavior, grounding the memory/planning/multi-agent-simulation pattern. Checked as of 2026-06-08. Citation role: curriculum_anchor. Source lane: agentic_ai_governance. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: source URL, DOI, edition/standard version, or claim scope materially changes. Verification method: direct_source_url_review. Claim scope: Backs the memory/planning/multi-agent simulation design pattern. Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.

Pezzulo G. & Friston K. J. Parr, T. Active inference: The free energy principle in mind, brain, and behavior, 2022. URL https://direct.mit.edu/books/oa-monograph/5299/Active-InferenceThe-Free-Energy-Principle-in-Mind. The open-access MIT Press monograph giving the book-length, chapter-organized foundational treatment of active inference, from the free-energy principle to discrete and continuous generative models and their behavioral implications. Checked as of 2026-06-08. Citation role: curriculum_anchor. Source lane: cognitive_active_inference. Source tier: scholarly_textbook. Refresh cadence: annual. Refresh trigger: source URL, DOI, edition/standard version, or claim scope materially changes. Verification method: direct_source_url_review. Claim scope: Chapter-level foundational reference for the active inference material across the AGEINT curriculum. Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.

Open Contracting Partnership. Open contracting data standard, 2026. URL https://standard.open-contracting.org/latest/en/. International open data standard for publishing public contracting data and documents across planning, tender, award, contract, and implementation stages. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: procurement_vendor_governance. Source tier: technical_standard. Refresh cadence: annual. Refresh trigger: OCDS schema, documentation version, governance page, or procurement transparency model changes. Verification method: direct_standards_page_review. Claim scope: procurement data lineage, vendor transparency, contracting records, and audit-ready disclosure. Stakeholder role: procurement analyst, auditor, vendor, civic reviewer, and instructor. Assurance use: contracting data schema and vendor record provenance check. Rights dimension: public transparency, accountability, anti-corruption, and access to information. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Zhang T. Wang X. & Gonzalez J. E. Patil, S. G. Gorilla: Large language model connected with massive apis, 2023. URL https://arxiv.org/abs/2305.15334. Verified scholarly preprint source for tool_use_agents; routed to Foundations of AGEINT (tool-use patterns); AGEINT Python Code Library; LangChain/LangGraph Patterns appendix. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: tool_use_agents. Source tier: scholarly_preprint. Refresh

cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for tool_use_agents materially changes. Verification method: direct_arxiv_record_review. Claim scope: Supports bounded AGEINT discussion of tool_use_agents and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that tool_use_agents claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_patil_2023_gorilla retained.

Christopher Paul and Miriam Matthews. The russian "firehose of falsehood" propaganda model (rand, 2016), 2016. URL https://www.rand.org/pubs/perspectives/PE198.html. Verified professional documentation source for active_measures_disinformation; routed to Active Measures and Disinformation; Information Warfare and Cognitive Security. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: active_measures_disinformation. Source tier: professional_documentation. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for active_measures_disinformation materially changes. Verification method: direct_source_url_review. Claim scope: Supports bounded AGEINT discussion of active_measures_disinformation and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that active_measures_disinformation claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_rand_paul_matthews_firehose_falsehood normalized to professional_rand_paul_matthews_firehose_falsehood.

Epstein Ziv Mosleh Mohsen et al. Pennycook, Gordon. Shifting attention to accuracy - nature, 2021. URL https://www.nature.com/articles/s41586-021-03344-2. Verified scholarly peer reviewed source for cognitive_security_misinformation; routed to Cognitive Security (psychological inoculation & prebunking); Cognitive Security Operations (scalable interventions). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: cognitive_security_misinformation. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for cognitive_security_misinformation materially changes. Verification method: direct_source_url_review. Claim scope: Supports bounded AGEINT discussion of cognitive_security_misinformation and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that cognitive_security_misinformation claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_pennycook_2021_accuracy_nudge_nature retained.

Gordon Pennycook and David G. Rand. The psychology of fake news (trends in cognitive sciences, 2021), 2021. URL https://pubmed.ncbi.nlm.nih.gov/33736957/. Verified scholarly repository record source for disinformation_cognitive_psychology; routed to Active Measures and Disinformation; Social Engineering; Information Warfare and Cognitive Security. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: disinformation_cognitive_psychology. Source tier: scholarly_repository_record. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for disinformation_cognitive_psychology materially changes. Verification method: direct_source_url_review. Claim scope: Supports bounded AGEINT discussion of disinformation_cognitive_psychology and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that disinformation_cognitive_psychology claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_pennycook_rand_2021_psychology_fake_news retained.

& Ribeiro I. Perez, F. Ignore previous prompt: Attack techniques for language models, 2022. URL https://arxiv.org/abs/2211.09527. Verified scholarly preprint source for adversarial_ai_security; routed to Security & Adversarial Considerations; ATT&CK & Kill Chain Templates appendix; Cognitive Security & Inoculation appendix. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: adversarial_ai_security. Source tier: scholarly_preprint. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for adversarial_ai_security materially changes. Verification method: direct_arxiv_record_review. Claim scope: Supports bounded AGEINT discussion of adversarial_ai_security and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that adversarial_ai_security claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_perez_2022_prompt_injection retained.

Katherine Hibbs Pherson; Randolph H. Pherson. Critical thinking for strategic intelligence, 2020. URL https://collegepublishing.sagepub.com/products/critical-thinking-for-strategic-intelligence-3-265236. SAGE/CQ Press textbook page for critical-thinking questions, analytic techniques, uncertainty, graphics, and source evaluation in intelligence education. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: analytic_method_pedagogy. Source tier: scholarly_textbook. Refresh cadence: annual. Refresh trigger: Publisher page, edition, ISBN, or access status changes. Verification method: publisher_page_review. Claim scope: Supports bounded claims about critical-thinking pedagogy, source evaluation, uncertainty communication, and analytic graphics rather than automated judgment replacement. Stakeholder role: curriculum designer; analytic tradecraft instructor; writing reviewer. Assurance use: Strengthens SAT-adjacent teaching language around critical questions, source evaluation, and accountable presentation. Rights dimension: copyrighted textbook metadata only; cite and summarize sparingly. SAGE College Publishing product page verified live 2026-06-15 for title, authors, third edition, publisher, date, ISBNs, and description.

Richards J. Heuer Jr.; Randolph H. Pherson. Structured analytic techniques for intelligence analysis, 2014a. URL https://us.sagepub.com/en-us/nam/structured-analytic-techniques-for-intelligence-analysis/book242171. The standard practitioner catalogue of fifty-five structured analytic techniques (e.g., Analysis of Competing Hypotheses, Key Assumptions Check, Devil's Advocacy) used to counter cognitive bias in intelligence analysis. Checked as of 2026-06-08. Citation role: curriculum_anchor. Source lane: analytic_tradecraft. Source tier: scholarly_textbook. Refresh cadence: annual. Refresh trigger: source URL, DOI, edition/standard version, or claim scope materially changes. Verification method: direct_source_url_review. Claim scope: Grounds the AGEINT structured-analytic-techniques (SAT) catalogue and definitions, supplying an authoritative primary anchor for the techniques enumerated in the curriculum. Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.

Sarah Miller Beebe; Randolph H. Pherson. Cases in intelligence analysis: Structured analytic techniques in action, 2014b. URL https://collegepublishing.sagepub.com/products/cases-in-intelligence-analysis-2-242321. SAGE/CQ Press textbook page for SAT case pedagogy and classroom exercises for analyst training. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: analytic_method_pedagogy. Source tier: scholarly_textbook. Refresh cadence: annual. Refresh trigger: Publisher page, edition, ISBN, or access status changes. Verification method: publisher_page_review. Claim scope: Supports bounded claims about SAT case pedagogy, technique templates, and classroom application rather than empirical technique efficacy. Stakeholder role: curriculum designer; analytic tradecraft instructor; pedagogy reviewer. Assurance use: Adds publisher-backed support for SAT classroom-artifact language and exercise design. Rights dimension: copyrighted textbook metadata only;

cite and summarize sparingly. SAGE College Publishing product page verified live 2026-06-15 for title, subtitle, authors, edition, publisher, date, ISBNs, and description.

Privacy and Civil Liberties Oversight Board. Oversight reports, 2026. URL https://www.pclob.gov/Oversight. Official oversight-report library for privacy, civil-liberties, surveillance, watchlisting, facial-recognition, and redress analysis. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: legal_oversight. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Agent2Agent Protocol Project. Agent2agent (a2a) protocol, 2025a. URL https://a2a-protocol.org/latest/. Official Agent2Agent (A2A) protocol documentation describing an open standard for AI agents to securely communicate, collaborate, and coordinate work. Checked as of 2026-06-06. Citation role: curriculum_anchor. Source lane: agent_interoperability_standards. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: A2A protocol version, agent-discovery model, security profile, transport model, or governance home changes. Verification method: direct_official_page_review. Claim scope: Agent2Agent protocol interoperability, agent discovery and communication, cross-agent collaboration, and secure multi-agent coordination assumptions. Stakeholder role: multi-agent system architect, interoperability reviewer, instructor, procurement assessor, and learner. Rights dimension: interoperability, security, transparency, accountability, and auditable multi-agent coordination. Direct source URL verified live (HTTP 200, official A2A protocol documentation with on-topic description metadata) for AGEINT curriculum use.

Model Context Protocol Project. Security best practices - model context protocol, 2025b. URL https://modelcontextprotocol.io/docs/tutorials/security/security_best_practices. Official MCP security best practices page describing security considerations, attack vectors, and implementation practices for MCP deployments. Checked as of 2026-06-11. Citation role: curriculum_anchor. Source lane: secure_release_change_control. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: MCP security guidance, authorization/security-best-practice page, confused-deputy mitigation, token-handling guidance, or tool-consent requirements change. Verification method: direct_official_page_review. Claim scope: MCP security best practices, confused-deputy and token-passthrough risks, human consent, least privilege, authorization boundaries, and agent-tool threat modeling. Stakeholder role: security architect, release reviewer, agent-platform engineer, instructor, and learner. Assurance use: MCP deployment threat model, confused-deputy mitigation checklist, token-handling review, human-consent gate, least-privilege scope, and release-gate security evidence. Rights dimension: security, consent, least privilege, credential protection, accountability, user control, and harm prevention. Direct official MCP security best-practices page verified live 2026-06-11; page describes security considerations, attack vectors, and best practices for MCP implementations.

Model Context Protocol Project. Specification - model context protocol, 2025c. URL https://modelcontextprotocol.io/specification/2025-06-18. Official Model Context Protocol specification page for the 2025-06-18 version, grounding agent-tool interoperability language and protocol-boundary examples. Checked as of 2026-06-11. Citation role: curriculum_anchor. Source lane: agent_interoperability_standards. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: MCP specification version, protocol capability model, authorization profile, transport guidance, or security model changes. Verification method: direct_official_page_review. Claim scope: Model Context Protocol specification, client-server-tool interoperability, capability negotiation, authorization boundaries, and agentic context integration assumptions. Stakeholder role: agent-platform engineer, interoperability reviewer, procurement assessor, instructor, and learner. Rights dimension: interoperability, transparency, least-privilege integration, tool accountability, auditable agent context exchange, and user consent. Direct official MCP specification page verified live 2026-06-11; security and trust language retained as a boundary, not a deployment guarantee.

Open Worldwide Application Security Project. Owasp top 10 for large language model applications, 2025d. URL https://owasp.org/www-project-top-10-for-large-language-model-applications/. Security taxonomy for prompt injection, excessive agency, data leakage, and LLM application risks. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: agentic_ai_governance. Source tier: security_standard. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

OWASP Foundation CycloneDX Project. Cyclonedx specification overview, 2026a. URL https://cyclonedx.org/specification/overview/. CycloneDX specification overview for bill-of-materials formats, used to ground component inventory, dependency provenance, and supplier evidence in agentic AI systems. Checked as of 2026-06-06. Citation role: curriculum_anchor. Source lane: model_data_provenance. Source tier: security_standard. Refresh cadence: quarterly. Refresh trigger: CycloneDX specification version, BOM type, vulnerability extension, AI/component metadata, or supply-chain provenance guidance changes. Verification method: direct_project_specification_review. Claim scope: software bill of materials, service and operations BOMs, vulnerability and dependency metadata, and supply-chain component provenance. Stakeholder role: supply-chain analyst, SBOM steward, procurement assessor, secure-release reviewer, instructor, and learner. Assurance use: component-inventory evidence, dependency-risk review, supplier BOM checklist, and release-gate provenance record. Rights dimension: transparency, supply-chain accountability, security, auditability, and user harm reduction. Direct source URL verified live (HTTP 200, official CycloneDX specification overview page) for AGEINT curriculum use.

OWASP GenAI Security Project. Owasp top 10 for agentic applications for 2026, 2026b. URL https://genai.owasp.org/resource/owasp-top-10-for-agentic-applications-for-2026/. OWASP GenAI Security Project resource identifying critical risks and mitigations for autonomous and agentic AI applications. Checked as of 2026-06-11. Citation role: curriculum_anchor. Source lane: agentic_ai_security. Source tier: security_standard. Refresh cadence: semiannual. Refresh trigger: OWASP Agentic Applications Top 10 version, risk category, mitigation guidance, or project URL changes. Verification method: direct_standards_page_review. Claim scope: Peer-reviewed OWASP security-risk taxonomy for autonomous and agentic AI applications, including agent-goal hijack, tool misuse, privilege abuse, supply-chain exposure, and inter-agent communication risk. Stakeholder role: security architect, red-team reviewer, release owner, instructor, and learner. Assurance use: agentic application risk taxonomy, tool-misuse review, identity-and-privilege checks, supply-chain checklist, and secure-release gate evidence. Rights dimension: security, least privilege, supply-chain integrity, safe tool use, accountable agent behavior, and harm prevention. Direct OWASP GenAI Security Project resource verified live 2026-06-11 with the 2026 Agentic Applications Top 10 scope and peer-reviewed security-risk framing.

Sigstore Project. Overview - sigstore, 2026c. URL https://docs.sigstore.dev/. Sigstore documentation overview for software signing and transparency-log backed artifact verification, used to ground tamper-evident release and provenance evidence. Checked as of 2026-06-06. Citation role: curriculum_anchor. Source lane: secure_release_change_control. Source tier: security_standard. Refresh cadence: quarterly. Refresh trigger: Sigstore documentation, signing workflow, transparency log, identity binding, provenance verification, or project governance changes. Verification method: direct_project_documentation_review. Claim scope: software signing, transparency logs, artifact identity, provenance verification, and tamper-evident release evidence. Stakeholder role: release signer, supply-chain security reviewer, procurement assessor, instructor, and learner. Assurance use: artifact-signing evidence, transparency-log verification, release authenticity check, and supply-chain audit trail. Rights dimension: security, transparency, accountability, provenance, and harm prevention. Direct source URL verified live (HTTP 200, official Sigstore documentation overview page) for AGEINT curriculum use.

Special Competitive Studies Project and Australian Strategic Policy Institute. The future of intelligence analysis: U.s.-australia project on ai and human-machine teaming, 2024. URL https://www.scsp.ai/wp-content/uploads/2024/09/AI-The-Future-of-Intelligence-Analysis-SCSP-ASPI-Report.pdf. SCSP/ASPI public report on AI and human-machine teaming for intelligence analysis, routed for governance, training, and analytic-workflow boundary discussion. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: ai_enabled_analysis_boundary. Source tier: public_domain_primary. Refresh cadence: annual. Refresh trigger: SCSP report URL, PDF, AI analytic-team recommendations, or public

policy context materially changes. Verification method: primary_browser_pdf_review. Claim scope: Supports bounded discussion of AI human-machine teaming for all-source analysis; forward-looking recommendations remain policy context, not AGEINT performance evidence. Stakeholder role: analytic manager, AI governance reviewer, instructor, alliance liaison educator. Assurance use: human-machine teaming review, analytic-workflow modernization caveats, and alliance-interoperability discussion. Rights dimension: human oversight, analytic accountability, alliance coordination, lawful use, and public trust. Direct SCSP report PDF was verified on 2026-06-15 through the current SCSP resource page after the attachment URL had moved.

Liang S. Ye Y. Zhu K. Yan L. Lu Y. Lin Y. Cong X. Tang X.-Qian B. Zhao S.-Tian R. Xie R. Zhou J. Gerstein M. Li D. Liu Z. & Sun M. Qin, Y. Toolllm: Facilitating large language models to master 16000+ real-world apis, 2023. URL https://arxiv.org/abs/2307.16789. Verified scholarly preprint source for tool_use_agents; routed to Foundations of AGEINT (tool-use); AGEINT Python Code Library; LangChain/LangGraph Patterns appendix. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: tool_use_agents. Source tier: scholarly_preprint. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for tool_use_agents materially changes. Verification method: direct_arxiv_record_review. Claim scope: Supports bounded AGEINT discussion of tool_use_agents and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that tool_use_agents claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_qin_2023_toolllm retained.

Michael. Quinlan. Just intelligence: Prolegomena - semantic scholar, 2007. URL https://www.semanticscholar.org/paper/Just-intelligence:-Prolegomena-to-an-ethical-theory-Quinlan/4b55eed16d59a1f2c103394b2ae0eef592af2728. Verified scholarly repository record source for ethics_of_intelligence; routed to Ethics of Intelligence and Cognitive Security; just-intelligence theory. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: ethics_of_intelligence. Source tier: scholarly_repository_record. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for ethics_of_intelligence materially changes. Verification method: direct_source_url_review. Claim scope: Supports bounded AGEINT discussion of ethics_of_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that ethics_of_intelligence claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_quinlan_2007_just_intelligence retained.

& Georgeff M. P. Rao, A. S. Bdi agents: From theory to practice, 1995. URL https://aaai.org/papers/icmas95-042-bdi-agents-from-theory-to-practice/. Verified scholarly repository record source for agent_foundations; routed to Foundations of AGEINT (agent architectures); Design Patterns & Archetypes (goal-directed agent archetypes). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: agent_foundations. Source tier: scholarly_repository_record. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for agent_foundations materially changes. Verification method: direct_source_url_review. Claim scope: Supports bounded AGEINT discussion of agent_foundations and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that agent_foundations claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_rao_georgeff_1995_bdi retained.

Ronald. Reagan. Eo 12333 - odni, 1981. URL https://www.odni.gov/files/NCSC/documents/Regulations/EO_12333.pdf. Verified official primary source for legal_authorities_intelligence_collection; routed to Legal Authorities and Constraints; EO-based authorities for IC collection. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: legal_authorities_intelligence_collection. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for legal_authorities_intelligence_collection materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of legal_authorities_intelligence_collection and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that legal_authorities_intelligence_collection claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_eo_12333_odni_text retained; stale or indirect proposal URL replaced with direct source record.

UNESCO Global Education Monitoring Report. Ai and education, 2026. URL https://www.unesco.org/gem-report/en/ai-and-education. Official UNESCO GEM source hub for AI and education evidence, policy, access, assessment, and equity analysis. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: education_assessment. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: GEM report, policy note, dashboard, or education indicator update. Verification method: direct_official_page_review. Claim scope: education evidence, access and equity, assessment policy, and AI literacy governance. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Yi R. Fung Khanh Duy Nguyen Qi Zeng Manling Li Ziqi Wang Clare Voss Revanth Gangi Reddy, Daniel Lee and Heng Ji. Smartbook: Ai-assisted situation report generation for intelligence analysts, 2023. URL https://arxiv.org/abs/2303.14337. SmartBook preprint describing AI-assisted situation-report generation for intelligence analysts, including source grounding, analyst preferences, and evaluation caveats relevant to generated-product review. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: ai_enabled_analysis_boundary. Source tier: scholarly_preprint. Refresh cadence: semiannual. Refresh trigger: arXiv version, published venue metadata, evaluation claims, or analyst-support literature materially changes. Verification method: direct_arxiv_page_review. Claim scope: Supports bounded discussion of AI-assisted situation-report generation and grounded summaries; reported study results are treated as source-specific, not AGEINT performance evidence. Stakeholder role: analyst, instructor, AI product reviewer, assurance evaluator. Assurance use: AI-assisted analytic product review, source-grounding checklist design, and classroom situation-report caveats. Rights dimension: source traceability, analyst comprehension, transparency, and non-automation of judgment. Direct arXiv source URL verified on 2026-06-15 with title, authors, abstract, version metadata, and DOI record visible on the primary page.

Tom Ritchey. General morphological analysis: A general method for non-quantified modelling, 2013. URL https://www.swemorph.com/ma.html. Swedish Morphological Society page explaining general morphological analysis as a method for structuring non-quantified complex problem spaces. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: analytic_method_pedagogy. Source tier: public_scholarly_method_note. Refresh cadence: annual. Refresh trigger: Method page, PDF, revision note, or licensing statement changes. Verification method: public_method_page_review. Claim scope: Supports bounded claims about morphological analysis as a structuring method for non-quantified multidimensional problems, not as analytic validation by itself. Stakeholder role: methods instructor; curriculum designer; visualization reviewer. Assurance use: Adds method-root support for morphological and scenario matrix exercises while preserving review gates. Rights dimension: public method page; cite source and avoid extended quotation. Swedish Morphological Society method page verified live 2026-06-15 for title, author, revision note, and method description; used as a public method source for Zwicky-derived morphological analysis.

& Norvig P. Russell, S. Artificial intelligence: A modern approach, 4th ed., 2020. URL https://aima.cs.berkeley.edu. Verified scholarly repository record source for agent_foundations; routed to Foundations of AGEINT (agent definition, PEAS framework, rational agents); AGEINT Python Code Library. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: agent_foundations. Source tier: scholarly_repository_record. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for agent_foundations materially changes. Verification method: direct_source_url_review. Claim scope: Supports bounded AGEINT discussion of agent_foundations and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that agent_foundations claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_russell_norvig_2020_aima retained.

Jane; Dessi Roberto; Raileanu Roberta; Lomeli Maria; Zettlemoyer Luke; Cancedda Nicola; Scialom Thomas Schick, Timo; Dwivedi-Yu. Toolformer: Language models can teach themselves to use tools, 2023. URL https://arxiv.org/abs/2302.04761. Shows an LLM self-supervising when and how to call external APIs (calculator, search, QA, translation, calendar), grounding the tool-use / API-calling pattern for agents. Checked as of 2026-06-08. Citation role: curriculum_anchor. Source lane: agentic_ai_governance. Source tier: scholarly_preprint. Refresh cadence: annual. Refresh trigger: source URL, DOI, edition/standard version, or claim scope materially changes. Verification method: direct_source_url_review. Claim scope: Backs the tool-use / API-calling design pattern. Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.

Paul Allan. Schott. World bank/imf reference guide to aml/cft (2006), 2006. URL https://documents.worldbank.org/en/publication/documents-reports/documentdetail/558401468134391014/reference-guide-to-anti-money-laundering-and-combating-the-financing-of-terrorism-second-edition-and-supplement-on-special-recommendation-ix. Verified official primary source for finint_aml_cft_international; routed to Financial Intelligence (FININT). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: finint_aml_cft_international. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for finint_aml_cft_international materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of finint_aml_cft_international and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that finint_aml_cft_international claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key official_worldbank_aml_reference_guide retained.

Government Digital Service. Guidance for organisations using the algorithmic transparency recording standard, 2025a. URL https://www.gov.uk/government/publications/guidance-for-organisations-using-the-algorithmic-transparency-recording-standard. Official guidance for completing and publishing ATRS records, including public-sector template support and repository submission expectations. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: algorithmic_transparency_reporting. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: ATRS completion guidance, repository process, or publication policy changes. Verification method: direct_official_page_review. Claim scope: transparency notice fields, publication workflow, model specification, and review records. Stakeholder role: public official, records steward, instructor, transparency reviewer, and learner. Assurance use: transparency notice field checklist and publication decision evidence. Rights dimension: public transparency, explainability, accessibility, data protection, and redress. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Government Digital Service. Algorithmic transparency recording standard hub, 2025b. URL https://www.gov.uk/government/collections/algorithmic-transparency-recording-standard-hub. Official UK hub for ATRS records, public-sector transparency expectations, mandatory-scope policy, template guidance, and publication support. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: algorithmic_transparency_reporting. Source tier: official_primary. Refresh cadence: quarterly. Refresh trigger: ATRS template, scope policy, central government mandate, or publication guidance changes. Verification method: direct_official_page_review. Claim scope: algorithmic transparency notices, public records, public-sector service disclosure, and exemptions. Stakeholder role: public official, transparency reviewer, instructor, affected community, and learner. Assurance use: transparency notice workflow and public accountability evidence. Rights dimension: access to information, public accountability, participation, privacy, and civic trust. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

Joint IDP Profiling Service. Technical brief on joint structured analysis techniques, 2021. URL https://www.jips.org/jips-publication/jointstructuredanalysistechniques-jsat-2021/. JIPS technical brief on joint structured analysis techniques for collaborative humanitarian and development data analysis. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: analytic_method_pedagogy. Source tier: public_practice_guidance. Refresh cadence: annual. Refresh trigger: JIPS publication page, PDF, date, or guidance metadata changes. Verification method: direct_publication_page_review. Claim scope: Supports bounded claims about collaborative SAT facilitation, dissent, uncertainty management, and technique selection in humanitarian analysis contexts. Stakeholder role: methods instructor; curriculum designer; collaborative-analysis facilitator. Assurance use: Broadens SAT pedagogy beyond intelligence-only settings while preserving domain and efficacy caveats. Rights dimension: public guidance page; cite source and avoid extended quotation. JIPS publication page verified live 2026-06-15 for title, authoring organization, date, purpose statement, and download link.

Federico; Berman Edward; Gopinath Ashwin; Narasimhan Karthik; Yao Shunyu Shinn, Noah; Cassano. Reflexion: Language agents with verbal reinforcement learning, 2023. URL https://arxiv.org/abs/2303.11366. Proposes agents that verbally reflect on task feedback and store reflections in episodic memory to improve on later trials, grounding the self-reflection and stop-condition pattern for iterative agents. Checked as of 2026-06-08. Citation role: curriculum_anchor. Source lane: agentic_ai_governance. Source tier: scholarly_preprint. Refresh cadence: annual. Refresh trigger: source URL, DOI, edition/standard version, or claim scope materially changes. Verification method: direct_source_url_review. Claim scope: Backs the self-reflection / stop-condition design pattern for iterative LLM agents. Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.

Linux Foundation SPDX Project. Spdx specification 3.0.1, 2024. URL https://spdx.github.io/spdx-spec/v3.0.1/. SPDX 3.0.1 specification for creating software bills of materials and related machine-readable provenance records; used to ground model/data/software documentation evidence. Checked as of 2026-06-06. Citation role: curriculum_anchor. Source lane: model_data_provenance. Source tier: technical_standard. Refresh cadence: annual. Refresh trigger: SPDX specification version, profile model, security/licensing field, SBOM practice, or Linux Foundation governance update changes. Verification method: direct_project_specification_review. Claim scope: software bill of materials, package and file metadata, licensing provenance, security and lifecycle profiles, and machine-readable supply-chain documentation. Stakeholder role: documentation steward, provenance reviewer, license/compliance assessor, instructor, and learner. Assurance use: SBOM/provenance field checklist, documentation-card evidence, licensing/security review, and audit-trail crosswalk. Rights dimension: transparency, accountability, licensing clarity, security, and auditability. Direct source URL verified live (HTTP 200, official SPDX Specification 3.0.1 page with SBOM description metadata) for AGEINT curriculum use.

Rastogi A. Rao A. Shoeb A. A. M. Abid A. Fisch A. Brown A. R. Santoro A. Gupta A. Garriga-Alonso A. et al. Srivastava, A. Beyond the imitation game: Quantifying and extrapolating the capabilities of llms, 2022. URL https://arxiv.org/abs/2206.04615. Verified scholarly preprint source

for llm_evaluation; routed to Frameworks & Infrastructure (model evaluation); Security & Adversarial Considerations; AGEINT Python Code Library. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: llm_evaluation. Source tier: scholarly_preprint. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for llm_evaluation materially changes. Verification method: direct_arxiv_record_review. Claim scope: Supports bounded AGEINT discussion of llm_evaluation and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that llm_evaluation claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_srivastava_2022_bigbench retained.

Ahmer Arif Starbird, Kate and Tom Wilson. Disinformation as collaborative work (acm cscw, 2019), 2019. URL https://dl.acm.org/doi/10.1145/3359229. Verified scholarly repository record source for active_measures_information_operations; routed to Active Measures and Disinformation; Information Warfare and Cognitive Security; Social Engineering. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: active_measures_information_operations. Source tier: scholarly_repository_record. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for active_measures_information_operations materially changes. Verification method: direct_source_url_review. Claim scope: Supports bounded AGEINT discussion of active_measures_information_operations and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that active_measures_information_operations claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_starbird_arif_wilson_2019_disinfo_collaborative retained.

Peter Svenmarck. Overview of structured analytic techniques for assessment and judgement of major events, 2021. URL https://foi.se/en/foi/reports/report-summary.html?reportNo=FOI-R--5116--SE. Swedish Defence Research Agency report summary on 42 structured analytic techniques for assessment and judgement of major events. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: analytic_method_pedagogy. Source tier: official_research_report. Refresh cadence: annual. Refresh trigger: FOI report page, report number, download link, or abstract metadata changes. Verification method: direct_official_report_page_review. Claim scope: Supports bounded claims that SAT catalogues are used in public-sector training contexts and classify techniques by purpose and facilitation needs. Stakeholder role: curriculum designer; public-sector method instructor; reviewer. Assurance use: Adds a non-US official SAT training reference while keeping efficacy claims separate from technique catalog coverage. Rights dimension: public official report summary; cite source and avoid extended quotation. FOI report-summary page verified live 2026-06-15 for title, author, report number FOI-R–5116–SE, date, abstract, and keywords.

Mariarosaria Taddeo and Luciano Floridi. Regulate artificial intelligence to avert cyber arms race, 2018. URL https://www.nature.com/articles/d41586-018-04602-6. Nature Comment article arguing for AI-cyber governance before escalation risks intensify, useful for high-level cyber policy and non-escalatory classroom framing. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: cyber_threat_intelligence. Source tier: scholarly_commentary. Refresh cadence: annual. Refresh trigger: Nature article URL, DOI metadata, or AI-cyber policy literature materially changes. Verification method: primary_browser_article_review. Claim scope: Supports bounded policy discussion of AI-enabled cyber escalation and arms-race risk; not technical guidance and not empirical AGEINT validation. Stakeholder role: policy reviewer, cyber instructor, governance analyst. Assurance use: AI-cyber escalation caveat, policy-risk review, and cyber-arms-race boundary setting. Rights dimension: non-escalation, public safety, accountability, proportionality, and international stability. Direct Nature article page was opened and verified on 2026-06-15 after the script fetch timed out; title, authors, date, and DOI were visible on the primary page.

Terp and Breuer. Disarm: A framework for analysis of disinformation campaigns, 2022. URL https://ieeexplore.ieee.org/document/9830669/. IEEE source on the DISARM framework for disinformation and influence operations, used for defensive taxonomy and reviewable incident mapping. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: cognitive_influence_security. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: IEEE record, DISARM framework version, influence-operation taxonomy, or defensive analysis practice materially changes. Verification method: script_http_200_scholarly_page_review. Claim scope: Supports defensive taxonomy and incident-analysis framing for influence operations; excludes persuasion campaign design, targeting, and manipulation guidance. Stakeholder role: cognitive-security analyst, instructor, incident reviewer. Assurance use: DISARM taxonomy review, defensive influence-incident mapping, and provenance checklist design. Rights dimension: transparency, public trust, freedom of expression, privacy, and defensive resilience. Direct IEEE source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

& Gardner Dan. Tetlock, Philip E. Superforecasting - google play books, 2015a. URL https://books.google.com/books/about/Superforecasting.html?id=ICgWrgEACAAJ. Verified scholarly book metadata source for analytic_tradecraft_forecasting; routed to Epistemic Rigor & Analytic Tradecraft (Advanced Analysis Methods); Good Judgment Project findings. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: analytic_tradecraft_forecasting. Source tier: scholarly_book_metadata. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for analytic_tradecraft_forecasting materially changes. Verification method: direct_publisher_or_catalog_record_review. Claim scope: Supports bounded AGEINT discussion of analytic_tradecraft_forecasting and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that analytic_tradecraft_forecasting claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_tetlock_gardner_2015_superforecasting retained; stale or indirect proposal URL replaced with direct source record.

Mandeep K. Dhami; David R. Mandel; Barbara A. Mellers; Philip E. Tetlock. Improving intelligence analysis with decision science, 2015b. URL https://doi.org/10.1177/1745691615598511. Peer-reviewed decision-science article connecting intelligence analysis improvement to forecasting, probability judgment, and uncertainty communication evidence. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: forecasting_calibration_evidence. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: Publisher metadata, DOI record, correction, or retraction status changes. Verification method: crossref_doi_metadata_review. Claim scope: Supports bounded claims that decision-science tools such as calibration, aggregation, and uncertainty communication complement SAT practice. Stakeholder role: forecasting instructor; evaluation lead; curriculum designer. Assurance use: Gives the SAT chapter an evidence complement beyond technique catalogues and postmortem lessons. Rights dimension: copyrighted scholarly article; cite DOI metadata and summarize sparingly. Crossref DOI metadata verified live 2026-06-15 for title, authors, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.

Philip E. Tetlock. Expert political judgment - internet archive, 2005. URL https://archive.org/details/expertpoliticalj0000tetl_u0t8. Verified scholarly book metadata source for analytic_tradecraft_forecasting; routed to Epistemic Rigor & Analytic Tradecraft (Advanced Analysis Methods); forecasting accuracy and calibration. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: analytic_tradecraft_forecasting. Source tier: scholarly_book_metadata. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for analytic_tradecraft_forecasting materially changes. Verification method: direct_publisher_or_catalog_record_review. Claim scope: Supports bounded AGEINT discussion of

analytic_tradecraft_forecasting and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that analytic_tradecraft_forecasting claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_tetlock_2005_expert_political_judgment retained.

Welton Chang; Elissabeth Berdini; David R. Mandel; Philip E. Tetlock. Restructuring structured analytic techniques in intelligence, 2018. URL https://doi.org/10.1080/02684527.2017.1400230. Peer-reviewed article arguing for a more evidence-attentive structuring of SATs and stronger links to judgment and decision-science research. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: sat_evaluation_evidence. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: Publisher metadata, DOI record, correction, or retraction status changes. Verification method: crossref_doi_metadata_review. Claim scope: Supports bounded claims that SAT pedagogy should externalize reasoning, specify mechanisms, and avoid unsupported broad debiasing claims. Stakeholder role: curriculum designer; analytic standards trainer; evaluation lead. Assurance use: Connects SAT chapter revisions to decision-science evidence and claim-calibration gates. Rights dimension: copyrighted scholarly article; cite DOI metadata and summarize sparingly. Crossref DOI metadata verified live 2026-06-15 for title, authors, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.

National Security Decision Directive 298 The White House. National operations security program, nsdd 298, 1988. URL https://www.reaganlibrary.gov/public/archives/reference/scanned-nsdds/nsdd298.pdf. National Security Decision Directive 298 establishing national operations security program policy, used as public historical doctrine context for defensive OPSEC governance. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: opsec_doctrine_governance. Source tier: official_primary. Refresh cadence: biennial. Refresh trigger: Reagan Library URL, public archive metadata, or official OPSEC historical-policy citation materially changes. Verification method: direct_official_pdf_review. Claim scope: Provides official historical OPSEC policy context for critical-information protection and public doctrine framing; not an operational OPSEC playbook. Stakeholder role: instructor, OPSEC reviewer, collection-governance reviewer. Assurance use: OPSEC doctrine provenance review, critical-information boundary setting, and defensive classroom governance. Rights dimension: lawful authority, source protection, public safety, records accountability, and evidence-bounded education. Direct Reagan Library PDF source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Briana Vecchione Jennifer Wortman Vaughan Hanna Wallach Hal Daume III Timnit Gebru, Jamie Morgenstern and Kate Crawford. Datasheets for datasets, 2021. URL https://arxiv.org/abs/1803.09010. Scholarly source for dataset documentation covering motivation, composition, collection process, recommended uses, communication, transparency, and accountability. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: dataset_documentation. Source tier: scholarly. Refresh cadence: annual. Refresh trigger: dataset documentation practice, data-card schema, or scholarly consensus changes. Verification method: direct_scholarly_page_review. Claim scope: dataset cards, lineage fields, collection context, recommended-use notes, and reuse constraints. Stakeholder role: data steward, dataset creator, instructor, learner, and downstream reviewer. Assurance use: dataset datasheet review and data lineage registry. Rights dimension: data transparency, accountable reuse, bias review, privacy, and affected-group visibility. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. Church committee final report (internet archive), 1976. URL https://archive.org/details/ChurchCommittee_FullReport. Verified public domain primary source for legal_oversight_intelligence; routed to Legal Authorities and Constraints; Historical Intelligence Services (American); oversight reform history. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: legal_oversight_intelligence. Source tier: public_domain_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for legal_oversight_intelligence materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of legal_oversight_intelligence and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that legal_oversight_intelligence claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key public_church_committee_1976_final_report retained.

U.S. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. Church committee final report book i: Foreign and military intelligence (s. rep. 94-755), Church Committeea. URL https://www.intelligence.senate.gov/sites/default/files/94755_I.pdf. Verified public domain primary source for humint_oversight_history; routed to HUMINT history and oversight; IC accountability; CI doctrine history. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: humint_oversight_history. Source tier: public_domain_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for humint_oversight_history materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of humint_oversight_history and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that humint_oversight_history claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key public_church_committee_book_i_1976 retained.

U.S. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. Church committee book iii: Nsa surveillance (s. rep. 94-755), Church Committeeb. URL https://www.aarclibrary.org/publib/church/reports/book3/pdf/ChurchB3_10_NSA.pdf. Verified public domain primary source for sigint_oversight_history; routed to SIGINT oversight history; NSA authorities and limitations; domestic surveillance doctrine. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: sigint_oversight_history. Source tier: public_domain_primary. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for sigint_oversight_history materially changes. Verification method: direct_official_url_review. Claim scope: Supports bounded AGEINT discussion of sigint_oversight_history and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that sigint_oversight_history claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key public_church_committee_book_iii_nsasurveillance_1976 retained.

NATO Allied Command Transformation. Alternative analysis handbook, 2017. URL https://www.act.nato.int/wp-content/uploads/2023/05/alta-handbook.pdf. Official NATO handbook presenting alternative-analysis techniques and facilitation practices for analytic teams. Checked as of 2026-06-11. Citation role: curriculum_anchor. Source lane: analytic_tradecraft_evidence. Source tier: official_alliance_guidance. Refresh cadence: annual. Refresh trigger: Refresh if NATO publishes a newer alternative-analysis handbook or relocates the PDF. Verification method: direct_pdf_download. Claim scope: Supports claims about alternative-analysis practice menus and facilitation, with empirical limits stated separately. Stakeholder role: analytic tradecraft instructor; team facilitator; curriculum designer. Assurance use: Provides official practice examples for alternative-analysis

workflows. Rights dimension: official alliance publication; cite handbook and avoid long excerpts. NATO ACT PDF verified live 2026-06-11; use as doctrine/practice guidance, not empirical proof of SAT effectiveness.

& Kahneman Daniel. Tversky, Amos. Judgment under uncertainty: Heuristics and biases, 1974. URL https://pubmed.ncbi.nlm.nih.gov/17835457/. Verified scholarly repository record source for cognitive_bias_foundations; routed to Cognitive Security (neurocognitive mechanisms); Epistemic Rigor & Analytic Tradecraft (cognitive bias in analysis). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: cognitive_bias_foundations. Source tier: scholarly_repository_record. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for cognitive_bias_foundations materially changes. Verification method: direct_source_url_review. Claim scope: Supports bounded AGEINT discussion of cognitive_bias_foundations and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that cognitive_bias_foundations claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_tversky_kahneman_1974_judgment_uncertainty retained.

Innovation UK Department for Science, Technology, and AI Safety Institute. Ai safety institute approach to evaluations, 2024. URL https://www.gov.uk/government/publications/ai-safety-institute-approach-to-evaluations/ai-safety-institute-approach-to-evaluations. Official evaluation guidance for advanced AI systems, including agent evaluations for tool use, semi-autonomy, and real-world actions. Checked as of 2026-05-21. Citation role: curriculum_anchor. Source lane: agentic_ai_governance. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: source URL, policy status, standard version, or legal text materially changes. Verification method: direct_source_url_review. Claim scope: curriculum grounding and source-backed synthesis. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

UNESCO. Recommendation on the ethics of artificial intelligence, 2021. URL https://www.unesco.org/en/artificial-intelligence/recommendation-ethics. Official UNESCO recommendation source for human rights, fairness, transparency, accountability, education, culture, environment, and governance. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: human_rights_governance. Source tier: international_standard. Refresh cadence: annual. Refresh trigger: UNESCO implementation guidance, monitoring tool, or recommendation resource changes. Verification method: direct_official_page_review. Claim scope: human-rights-based AI governance, ethics education, accountability, and societal impact. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

UNESCO. Guidance for generative ai in education and research, 2023. URL https://unesdoc.unesco.org/ark:/48223/pf0000386693. Official UNESCO publication for generative AI education governance, assessment integrity, age safeguards, teacher roles, and research use. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: education_assessment. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: UNESCO education guidance, generative-AI policy, or assessment recommendations change. Verification method: direct_publication_page_review. Claim scope: education policy, classroom AI governance, assessment integrity, and learner protection. Direct source URL verified against an official, standards, public-domain, or scholarly source for AGEINT curriculum use.

UNESCO. Ai competency frameworks for teachers and students, 2024. URL https://www.unesco.org/en/articles/unesco-launches-ai-competency-frameworks-students-and-teachers. Official UNESCO source for AI competency frameworks supporting teacher development, student capabilities, ethics, and curriculum design. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: education_assessment. Source tier: official_primary. Refresh cadence: annual. Refresh trigger: UNESCO framework publication, competency revision, or education resource update. Verification method: direct_official_page_review. Claim scope: teacher facilitation, learner competencies, assessment design, and AI literacy outcomes. Direct source URL verified against an official UNESCO source for AGEINT curriculum use as of 2026-05-22; automated liveness sweep on 2026-06-06 found the old article URL moved and recorded this likely successor URL, but UNESCO reset automated retrieval, so manual browser re-verification remains required.

European Union. Regulation (eu) 2024/1689: Artificial intelligence act, 2024. URL https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng. Official EU Artificial Intelligence Act legal text. Checked as of 2026-05-21. Citation role: source_quality_anchor. Source lane: source_quality_spine. Source tier: source_quality_anchor. Refresh cadence: semiannual. Refresh trigger: source version, legal status, standard revision, or official guidance changes. Verification method: direct_source_url_review. Claim scope: baseline source-quality guardrail for generated AGEINT curriculum claims. Stakeholder role: curriculum maintainer, instructor, reviewer, and learner. Assurance use: source-quality triangulation and claim-boundary review. Rights dimension: source transparency, accountability, and evidence traceability. Directly verified official EU source URL.

Institute in Macau United Nations University. Why agentic ai needs boundaries before freedom, 2026. URL https://unu.edu/macau/blog-post/why-agentic-ai-needs-boundaries-freedom. UNU Macau policy analysis arguing agentic AI requires boundaries before freedom - minimum necessary privilege, delimited scope, sandboxes, explicit permissions, and accountable oversight. Checked as of 2026-05-22. Citation role: curriculum_anchor. Source lane: human_rights_governance. Source tier: official_primary. Refresh cadence: semiannual. Refresh trigger: UNU Macau agentic-AI governance publications, minimum-privilege doctrine, oversight guidance, or UN academic agentic-AI policy changes. Verification method: direct_official_page_review. Claim scope: agentic AI governance, minimum necessary privilege, bounded scope, accountable oversight, and well-governed agency over maximal autonomy. Stakeholder role: AI governance steward, oversight reviewer, instructor, policy analyst, and learner. Assurance use: bounded-autonomy boundary review, minimum-necessary-privilege checklist, oversight-and-accountability map, and governance-design rationale. Rights dimension: accountability, public trust, human oversight, institutional values alignment, and harm prevention. Direct source URL verified live (HTTP 200, on-topic UNU Macau agentic-AI governance analysis) for AGEINT curriculum use.

National Institute of Standards U.S. AI Safety Institute and Technology. Managing misuse risk for dual-use foundation models, nist ai 800-1 initial public draft, 2024. URL https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.800-1.ipd.pdf. NIST AI 800-1 initial public draft on managing misuse risk for dual-use foundation models; used as draft official guidance, not as finalized regulation. Checked as of 2026-06-06. Citation role: curriculum_anchor. Source lane: ai_red_team_assurance. Source tier: official_draft. Refresh cadence: quarterly. Refresh trigger: NIST AI 800-1 finalization, draft revision, U.S. AI Safety Institute misuse-risk framework, dual-use foundation-model safeguard guidance, or evaluation practice changes. Verification method: direct_official_pdf_review. Claim scope: dual-use foundation-model misuse-risk management, safeguards, evaluation planning, governance roles, and draft-status caveats for frontier-model assurance. Stakeholder role: AI safety evaluator, red-team reviewer, release-gate owner, instructor, and learner. Assurance use: dual-use misuse-risk assessment, safeguard-evidence review, release-gate critique, and frontier-model red-team scope planning with draft-status caveat. Rights dimension: safety, misuse prevention, accountability, evaluation validity, incident readiness, and harm reduction. Direct source URL verified live (HTTP 200 PDF, title metadata and first pages on-topic); Draft status retained explicitly for AGEINT curriculum use.

& Tabarez Rienzi Fernando. Van Puyvelde, Damien. The rise of open-source intelligence, ejis 2025, 2025. URL https://www.cambridge.org/core/journals/european-journal-of-international-security/article/rise-of-opensource-intelligence/21122432399ECB8078BF0D89A76D0586. Verified scholarly repository record source for osint_methodology; routed to OSINT definition and discipline; OSINT methodology; validation and verification; civil society OSINT. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: osint_methodology. Source tier: scholarly_repository_record. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for osint_methodology materially changes. Verification method: direct_source_url_review. Claim scope: Supports bounded AGEINT discussion of osint_methodology and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures.

Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that osint_methodology claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_van_puyvelde_2025_rise_osint retained.

Shazeer N. Parmar N. Uszkoreit J. Jones L. Gomez A. N. Kaiser . & Polosukhin I. Vaswani, A. Attention is all you need, 2017. URL https://arxiv.org/abs/1706.03762. Verified scholarly preprint source for llm_architecture; routed to Foundations of AGEINT (LLM substrate); LangChain/LangGraph Patterns appendix; CrewAI appendix; AutoGen/MCP appendix. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: llm_architecture. Source tier: scholarly_preprint. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for llm_architecture materially changes. Verification method: direct_arxiv_record_review. Claim scope: Supports bounded AGEINT discussion of llm_architecture and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that llm_architecture claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_vaswani_2017_attention retained.

& Stickgold R. Walker, M. P. Sleep, memory, and plasticity, 2006. URL https://walkerlab.berkeley.edu/reprints/Walker&Stickgold_AnnRevPsych_2006.pdf. Verified scholarly repository record source for cognitive_performance; routed to Productivity Intelligence & Cognitive Performance (sleep and cognition); Cognitive Security & Inoculation appendix. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: cognitive_performance. Source tier: scholarly_repository_record. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for cognitive_performance materially changes. Verification method: direct_source_url_review. Claim scope: Supports bounded AGEINT discussion of cognitive_performance and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that cognitive_performance claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_walker_stickgold_2006_sleep_memory retained.

Claire Wardle and Hossein Derakhshan. Information disorder: Toward an interdisciplinary framework for research and policy making, 2017. URL https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c. Council of Europe report providing an interdisciplinary framework for information disorder, routed as terminology and source-provenance support for defensive cognitive-security lessons. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: cognitive_influence_security. Source tier: public_domain_primary. Refresh cadence: annual. Refresh trigger: Council of Europe PDF URL, information-disorder terminology, or platform-governance literature materially changes. Verification method: direct_public_pdf_review. Claim scope: Supports taxonomy and terminology for information disorder, misinformation, disinformation, and malinformation; does not authorize manipulation or counter-propaganda practice. Stakeholder role: media-literacy instructor, cognitive-security reviewer, policy analyst. Assurance use: information-disorder taxonomy review, provenance checklist design, and cognitive-security rights caveats. Rights dimension: freedom of expression, public trust, media literacy, privacy, and non-censorial resilience education. Direct Council of Europe source URL returned HTTP 200 on 2026-06-15 and was deduped against existing AGEINT anchors and source-guide references.

Xuezhi; Schuurmans Dale; Bosma Maarten; Ichter Brian; Xia Fei; Chi Ed; Le Quoc; Zhou Denny Wei, Jason; Wang. Chain-of-thought prompting elicits reasoning in large language models, 2022. URL https://arxiv.org/abs/2201.11903. Shows that prompting an LLM to emit intermediate reasoning steps markedly improves complex reasoning, establishing the reasoning-decomposition pattern that underlies agent planning and ReAct-style traces. Checked as of 2026-06-08. Citation role: curriculum_anchor. Source lane: agentic_ai_governance. Source tier: scholarly_preprint. Refresh cadence: annual. Refresh trigger: source URL, DOI, edition/standard version, or claim scope materially changes. Verification method: direct_source_url_review. Claim scope: Backs the reasoning-decomposition design pattern. Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.

Tim. Weiner. Legacy of ashes: The history of the cia, 2007. URL https://www.penguinrandomhouse.com/books/188076/legacy-of-ashes-by-tim-weiner/. Verified scholarly book metadata source for intelligence_history_american; routed to Historical Intelligence Services (American); CIA institutional failures and analytic dysfunction. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: intelligence_history_american. Source tier: scholarly_book_metadata. Refresh cadence: annual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for intelligence_history_american materially changes. Verification method: direct_publisher_or_catalog_record_review. Claim scope: Supports bounded AGEINT discussion of intelligence_history_american and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that intelligence_history_american claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_weiner_2007_legacy_ashes retained; stale or indirect proposal URL replaced with direct source record.

L. Weng. Llm-powered autonomous agents, 2023. URL https://lilianweng.github.io/posts/2023-06-23-agent/. Verified professional documentation source for agentic_design_principles; routed to Foundations of AGEINT (agent memory, tool use, planning); Design Patterns & Archetypes. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: agentic_design_principles. Source tier: professional_documentation. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for agentic_design_principles materially changes. Verification method: direct_professional_documentation_review. Claim scope: Supports bounded AGEINT discussion of agentic_design_principles and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that agentic_design_principles claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_weng_2023_agent_survey normalized to professional_weng_2023_agent_survey.

Martha Whitesmith. The efficacy of ach in mitigating serial position effects and confirmation bias in an intelligence analysis scenario, 2019. URL https://doi.org/10.1080/02684527.2018.1534640. Peer-reviewed ACH experiment used to keep confirmation-bias and serial-position claims specific to a study design rather than a general SAT guarantee. Checked as of 2026-06-15. Citation role: curriculum_anchor. Source lane: sat_evaluation_evidence. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: Publisher metadata, DOI record, correction, or retraction status changes. Verification method: crossref_doi_metadata_review. Claim scope: Supports bounded claims about ACH evidence for bias mitigation under a specific intelligence-analysis scenario. Stakeholder role: curriculum designer; analytic standards trainer; cognition reviewer. Assurance use: Prevents ACH lessons from turning one experimental result into a universal debiasing assertion. Rights dimension: copyrighted scholarly article; cite DOI metadata and summarize sparingly. Crossref DOI metadata verified live 2026-06-15 for title, author, journal DOI, publisher, and year; DOI URL retained as stable scholarly source.

James J. Wirtz. Are intelligence failures still inevitable?, 2023. URL https://www.tandfonline.com/doi/full/10.1080/08850607.2023.2214328. Peer-reviewed discussion revisiting intelligence-failure inevitability in light of collection, analysis, reform, and policy factors. Checked as of 2026-06-11. Citation role: curriculum_anchor. Source lane: intelligence_failure_postmortem. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: Refresh if publisher metadata, correction, or retraction status changes. Verification method: doi_metadata_review. Claim scope: Supports current failure-theory framing that reform can improve systems without eliminating surprise or policy-analysis friction. Stakeholder role: curriculum designer; governance reviewer; analytic standards trainer. Assurance use: Links classic failure theory to contemporary reform and warning lessons. Rights dimension: copyrighted scholarly article; cite DOI metadata and summarize sparingly. DOI/publisher URL retained; scholarly metadata verified live 2026-06-11 from DOI-indexed search results because automated publisher retrieval was rate-limited.

Roberta Wohlstetter. Pearl harbor: Warning and decision, 1962. URL https://www.sup.org/books/history/pearl-harbor. Publisher record for Wohlstetter's classic warning-intelligence study of signal, noise, and surprise before Pearl Harbor. Checked as of 2026-06-11. Citation role: curriculum_anchor. Source lane: warning_intelligence. Source tier: scholarly_publisher_record. Refresh cadence: annual. Refresh trigger: Refresh if publisher metadata or edition details change. Verification method: publisher_record_review. Claim scope: Supports historical warning-intelligence claims about signal-noise and surprise analysis. Stakeholder role: curriculum designer; intelligence history instructor. Assurance use: Frames warning lessons around indicators, noise, and uncertainty rather than hindsight certainty. Rights dimension: copyrighted scholarly book metadata only; do not reproduce extended text. Stanford University Press publisher page verified live 2026-06-11; use as classic warning theory, not as current doctrine.

Michael Wooldridge. An introduction to multiagent systems, 2nd edition, 2009. URL https://www.wiley.com/en-us/An+Introduction+to+MultiAgent+Systems%2C+2nd+Edition-p-9780470519462. Standard graduate textbook on multi-agent systems covering coordination, negotiation, voting, and auctions, grounding the multi-agent-coordination vocabulary used in agentic governance. Checked as of 2026-06-08. Citation role: curriculum_anchor. Source lane: agentic_ai_governance. Source tier: scholarly_textbook. Refresh cadence: annual. Refresh trigger: source URL, DOI, edition/standard version, or claim scope materially changes. Verification method: direct_source_url_review. Claim scope: Backs multi-agent coordination concepts and vocabulary. Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.

Nicholas R. Wooldridge, Michael; Jennings. Intelligent agents: theory and practice, 1995. URL https://www.cambridge.org/core/product/identifier/S0269888900008122/type/journal_article. Foundational survey dividing agent research into theory, architectures, and languages, providing the canonical agent definition and multi-agent-systems vocabulary that predates the LLM era. Checked as of 2026-06-08. Citation role: curriculum_anchor. Source lane: agentic_ai_governance. Source tier: scholarly_peer_reviewed. Refresh cadence: annual. Refresh trigger: source URL, DOI, edition/standard version, or claim scope materially changes. Verification method: direct_source_url_review. Claim scope: Backs the foundational agent definition and MAS vocabulary. Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.

Bansal G. Zhang J. Wu Y. Li B. Zhu E. Jiang L. Zhang X. Zhang S. Liu J. Awadallah A. H. White R. W. Burger D. & Wang C. Wu, Q. Autogen: Enabling next-gen llm applications via multi-agent conversation, 2023. URL https://arxiv.org/abs/2308.08155. Verified scholarly preprint source for multi_agent_frameworks; routed to AutoGen and MCP Patterns appendix; Frameworks & Infrastructure; CrewAI appendix (comparison context). AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: multi_agent_frameworks. Source tier: scholarly_preprint. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for multi_agent_frameworks materially changes. Verification method: direct_arxiv_record_review. Claim scope: Supports bounded AGEINT discussion of multi_agent_frameworks and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that multi_agent_frameworks claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_wu_2023_autogen retained.

Jeffrey; Yu Dian; Du Nan; Shafran Izhak; Narasimhan Karthik; Cao Yuan Yao, Shunyu; Zhao. React: Synergizing reasoning and acting in language models, 2023a. URL https://arxiv.org/abs/2210.03629. Introduces the interleaved reason-then-act loop in which an LLM alternates verbal reasoning traces with tool/environment actions, grounding the reason-act/tool-use pattern at the core of modern agent design. Checked as of 2026-06-08. Citation role: curriculum_anchor. Source lane: agentic_ai_governance. Source tier: scholarly_preprint. Refresh cadence: annual. Refresh trigger: source URL, DOI, edition/standard version, or claim scope materially changes. Verification method: direct_source_url_review. Claim scope: Backs the reason-act/tool-use design pattern, replacing a secondary blog/LinkedIn discussion with the canonical primary source. Direct source URL verified 2026-06-08 against the primary scholarly or standards source for AGEINT curriculum grounding.

Yu D. Zhao J. Shafran I. Griffiths T. L. Cao Y. & Narasimhan K. Yao, S. Tree of thoughts: Deliberate problem solving with llms, 2023b. URL https://arxiv.org/abs/2305.10601. Verified scholarly preprint source for agentic_reasoning; routed to Foundations of AGEINT (reasoning architectures); Design Patterns & Archetypes (planning patterns); LangChain/LangGraph Patterns appendix. AGEINT uses it for defensive, historical, governance, or method context, not for operational execution. Checked as of 2026-06-16. Citation role: curriculum_anchor. Source lane: agentic_reasoning. Source tier: scholarly_preprint. Refresh cadence: semiannual. Refresh trigger: source URL, source status, edition/version, or claim-scope boundary for agentic_reasoning materially changes. Verification method: direct_arxiv_record_review. Claim scope: Supports bounded AGEINT discussion of agentic_reasoning and related source evidence. It does not authorize collection tasking, exploit steps, covert-action guidance, manipulation playbooks, unsafe cyber-physical actions, or live-target procedures. Stakeholder role: instructor, analyst, reviewer, and curriculum maintainer. Assurance use: Checks that agentic_reasoning claims stay source-backed, bounded, and separated from operational practice. Rights dimension: public-source education, accountable review, privacy/civil-liberties awareness, and evidence-bounded safety boundary. Direct source URL reviewed on 2026-06-16; original proposal key scholarly_yao_2023_tree_of_thoughts retained.