



AF 9500

Aerospace Digital Systems,
Software &
Cybersecurity

Space / Aviation / Defense

FIRST EDITION

Document identity and authority

FIRST EDITION MANUSCRIPT - Prepared for Aerospace Federation review

Field	Declared position
Identifier	AF 9500
Title	Aerospace Digital Systems, Software & Cybersecurity
Organization	Aerospace Federation
Edition / language	FIRST EDITION / English master text
Content	Clauses 0-40 and Annexes A-T
Normative basis	Main clauses and Annexes A-N contain proposed requirements; Annexes O-T are informative.
Publication status	Review manuscript. Publication approval and effective date are not assigned.

Use of this publication

AF 9500 connects intended aerospace digital behavior, software lifecycle integrity, cybersecurity, valid evidence and authorized use. It addresses accidental faults, intentional misuse and the operational effects of protective controls. Product-specific values, architectures, permissions and authorities are completed for the actual application.

The supporting set provides original implementation models, technical profiles, examination checklists and blank controlled records. It does not supply fabricated results, signatures, approvals or recognition.

Informative calculations and cases use synthetic values. They explain assumptions, reproducible methods and decision boundaries; they are not mandatory defaults or evidence from actual systems.

Reader route and decision boundaries

1 Define the object and consequences

Use Clauses 0-8 and Annexes A-D for scope, authority, assets, classification, safety-security interactions, requirements and architecture.

2 Control development and evidence

Use Clauses 9-17 and Annexes D-F for lifecycle, suppliers, configuration, code, builds, tools, verification and timing.

3 Establish trustworthy operation

Use Clauses 18-24 and Annexes G-H for identity, cryptography, data, communication, platforms, cloud and industrial environments.

4 Apply the actual aerospace context

Select Clauses 25-28 and Annex K for aviation, space, remote missions, trained models and AI-assisted or agentic work.

5 Deploy, monitor, respond and recover

Use Clauses 29-35 and Annexes H-J for readiness, updates, detection, vulnerabilities, incidents, recovery and human operations.

6 Release, support and maintain claims

Use Clauses 36-40 and Annexes L-N for assurance cases, legacy use, retirement, records and publication or adoption.

Decision boundary: Build success, authentic content, accepted verification, risk acceptance, release and operating permission are distinct. An unresolved essential condition cannot be compensated for by an aggregate score.

Contents - clauses and annexes

Entries and PDF bookmarks locate the controlled clauses and annexes. Page references apply to this file.

0 Introduction and intended outcomes	8
1 Scope and lifecycle coverage	9
2 Applicability, precedence and local parameters	9
3 Terms and interpretation	11
4 Governance, competence and retained authority	12
5 System context, assets and consequence classification	12
6 Integrated safety, security and threat assessment	13
7 Requirements, interfaces and bidirectional traceability	14
8 Architecture, isolation and resilient behavior	14
9 Lifecycle planning, reviews and independent assurance	15
10 Suppliers, reusable software and dependency transparency	16
11 Configuration, baseline and change control	17
12 Software design, implementation and code review	17
13 Build environments, delivery pipelines and artifact provenance	18
14 Tool assurance, models and formal methods	19
15 Verification and validation strategy	19
16 Coverage, test data and anomaly disposition	20
17 Timing, concurrency and resource integrity	21
18 Identity, authentication and privileged access	21
19 Cryptography, key lifecycle and trust services	22
20 Data integrity, privacy and information handling	23

21 Communications, interfaces and distributed-system behavior	23
22 Platform, firmware and hardware-rooted trust	24
23 Cloud services, virtualization and shared infrastructure	25
24 Industrial, test and maintenance digital environments	26
25 Airborne and aviation ground-system integration	26
26 Space, remote mission and intermittent-link systems	27
27 Machine learning, trained models and adaptive functions	28
28 AI-assisted development and agentic tools	28
29 Hardening, secure configuration and deployment readiness	29
30 Updates, offline delivery and rollback control	30
31 Logging, detection and operational monitoring	30
32 Vulnerability intake, applicability and remediation	31
33 Incident response, evidence preservation and communication	32
34 Backup, recovery and operational continuity	32
35 Human interfaces, remote support and operational competence	33
36 Assurance case, release and truthful claims	34
37 Legacy systems, obsolescence and continuing support	34
38 Retirement, transfer and secure disposal	35
39 Assurance reviews, metrics and evidence continuity	36
40 Publication, local adoption and maintenance	36
Annex A - Activity-based applicability and retained duties	38
Annex B - Mandatory parameter baseline and common record payload	39
Annex C - Context, classification and integrated risk dossier	42

Annex D - Requirements, interfaces and traceability payload	43
Annex E - Supply, dependency and provenance dossier	44
Annex F - Verification, tool and anomaly evidence	45
Annex G - Identity, cryptography and trust-control records	46
Annex H - Deployment, update and rollback dossier	47
Annex I - Monitoring, vulnerability and incident records	48
Annex J - Recovery, continuity and state reconciliation	49
Annex K - Machine-learning and AI-assisted-work dossier	50
Annex L - Release, continued use and declaration payload	51
Annex M - Retirement, data disposition and evidence preservation	52
Annex N - Assurance, publication and local-adoption dossier	53
Annex O - Reproducible calculations and decision examples	54
Annex P - Integrated application cases	58
Annex Q - Digital assurance and decision diagrams	60
Annex R - Activity-based implementation routes	65
Annex S - Interpretation questions and boundary examples	67
Annex T - Requirement families and implementation crosswalk	69

Tables - requirements and worked evidence

Table 0-1. Digital decision boundaries	8
Table 3-1. Terms used by AF 9500	11
Table A-1. Activity triggers and primary clauses	38
Table B-1. P01-P44 parameter schedule	39
Table C-1. Hazard-threat scenario payload	42
Table D-1. Traceability minimum content	43
Table E-1. Build and release provenance	44
Table H-1. Required update transition evidence	47
Table I-1. Incident and evidence minimum content	48
Table L-1. Bounded digital release content	51
Table P-1. Example populated decision record for Case P.1	59
Table T-1. Core navigation map	69

0 Introduction and intended outcomes

0.1 Digital assurance chain

AF 9500 establishes requirements for aerospace digital systems, software and cybersecurity across development, acquisition, integration, operation, maintenance and retirement. Its purpose is a defensible connection between intended behavior, actual implementation, protection against misuse, valid evidence and authorized use. It covers space, aviation and defense applications without assigning a universal architecture or assurance level. The organization shall preserve the chain from system context and consequences to requirements, design, source and dependencies, built artifacts, deployed configuration and operational feedback. Evidence shall identify the exact object and conditions that it represents.

0.2 Distinct decisions

A successful build establishes that a defined build operation completed. A valid signature establishes an authenticated relationship to signed content under a specified trust policy. Neither alone establishes correct behavior, acceptable risk, compatibility or permission to operate. Verification, risk acceptance, product release and operational authorization shall be distinct recorded decisions.

Table 0-1. Digital decision boundaries

Decision	Required basis	What it does not establish
Build completion	Identified inputs, environment and resulting artifact.	Correctness or fitness for flight or mission use.
Verification acceptance	Valid evidence against exact requirements.	Approval of an untested environment or change.
Security risk acceptance	Explicit scenario, residual exposure, owner and conditions.	Removal of an unmet mandatory requirement.
Release and deployment	Reconciled evidence and authorized target population.	Universal approval of every installation or operation.

0.3 Evidence and state

The organization shall retain unsuccessful, adverse and inconclusive results. PASS, FAIL, HOLD and approved N/A shall remain distinguishable from workflow completion. A favorable aggregate score shall not override an unresolved essential safety, security or mission condition. An assumption that becomes false shall reopen dependent conclusions.

0.4 Language and publication status

Shall identifies a proposed requirement; should identifies guidance; may identifies permission within stated conditions. Informative examples explain methods and do not assign product-specific limits. This FIRST EDITION manuscript is prepared for Aerospace Federation review. Publication approval and effective date are not assigned. Publication, local adoption, certification and permission to operate remain separate actions.

Required evidence: A declared scope, controlled definitions, decision states, evidence relationships and publication or adoption authority.

Decision control: A document, score, signature or tool result shall not be represented as a broader technical decision than its actual evidence and authority support.

1 Scope and lifecycle coverage

1.1 Covered objects

This standard applies to embedded and hosted software, firmware, programmable logic interfaces, mission applications, command and control services, engineering tools, digital twins, data services, industrial systems and supporting infrastructure where they affect aerospace outcomes. It includes supplied and reused components, open-source dependencies, remotely hosted services and machine-learning functions. The scope shall identify each product, service, site, operator, owner and retained outsourced duty. Hardware and physical processes shall be included to the extent necessary to establish trustworthy digital behavior and interfaces.

1.2 Covered activities

Activities include concept definition, requirements, design, implementation, build, integration, verification, release, deployment, maintenance, vulnerability handling, incident response, recovery, transfer and retirement. A component supplier shall communicate limitations that an integrator needs to establish intended-use suitability. An operator shall assess deployment and continuing-use conditions even when development is outsourced.

1.3 Operational environments

Applicability shall address airborne, ground, space, maritime-support and industrial contexts as actually present. Disconnected operation, intermittent communications, limited compute resources, long support lives, maintenance access and contested conditions shall be explicit where relevant. A public-cloud business application and a flight-control function require different technical arguments even when they share lifecycle controls.

1.4 Boundaries

The standard does not itself grant airworthiness, launch, spectrum, military, data-processing or operating permissions. The organization shall identify applicable obligations and contractual requirements and resolve conflicts before reliance. Cybersecurity conformity shall not substitute for system safety, physical qualification or the operator's authorization. Claims shall identify the bounded object and activity assessed.

Required evidence: System and organizational scope, lifecycle map, environment description, retained duties and required permissions.

Decision control: A narrow component claim shall not be promoted to approval of an integrated vehicle, mission or enterprise without the necessary additional evidence.

2 Applicability, precedence and local parameters

2.1 Activity selection

The scope owner shall apply Annex A to actual activities and consequences. Shared controls remain applicable to outsourced work where responsibility is retained. Non-applicability shall identify an absent activity or condition, supporting facts, eligible approval and review trigger. Missing competence, access or evidence is a gap, not N/A.

2.2 Requirement precedence

The organization shall identify authoritative product requirements, contracts, permissions and interface agreements. Conflicting requirements shall be recorded with affected objects, responsible authorities and resolution. Procurement shorthand or a local template shall not silently weaken a technical requirement. Dependent work shall remain restricted until decision-sensitive conflicts are resolved.

2.3 Mandatory parameter baseline

Annex B defines P01-P44, which shall be completed by approved values or controlled references before dependent work. Parameters shall identify owners, units where relevant, applicability, source, effectivity and change triggers. A value may be a structured rule, model, boundary or matrix. Unsupported example values shall not become defaults.

2.4 Tailoring and equivalence

Alternative controls shall demonstrate that the original objective and necessary evidence strength are preserved. The proposal shall address consequence, coverage, independence, uncertainty and downstream reliance. Eligible approval shall identify exact scope and limitations. Tailoring shall not waive a required physical behavior, legal permission or safety constraint merely because a particular implementation is inconvenient.

Required evidence: Applicability decisions, precedence records, completed P01-P44 baseline and justified alternative-control approvals.

Decision control: Blank thresholds, unknown boundaries and unresolved essential dependencies shall block the affected acceptance, release or deployment decision.

3 Terms and interpretation

3.1 Core terms

Table 3-1. Terms used by AF 9500

Term	Meaning within this standard
Digital object	Identified software, firmware, data, model, service or configured platform under assurance.
Baseline	A controlled set of objects and their relationships for a defined purpose and time.
Trust boundary	An interface across which identity, authority, assumptions or protection conditions change.
Safety-security interaction	A situation where a threat or protective control can alter a safety-related outcome.
Build provenance	Evidence linking an artifact to its actual source, dependencies, tools, environment and build actions.
SBOM	Software bill of materials describing identified components and dependency relationships for a stated artifact and scope.
Recovery objective	An approved target for restoration time, recoverable state or permitted data loss.
Compensating control	A justified temporary or alternative measure with demonstrated coverage and explicit limitations.

3.2 Identity and configuration

An artifact shall have a stable identifier and version or digest as appropriate. Identity shall distinguish source, executable, configuration, trained model, data and deployed instance. A filename, product label or version string alone may be insufficient to establish the actual bytes or configuration. Identical bytes do not necessarily imply identical behavior under different platforms, permissions or inputs.

3.3 Decision states

PASS means that an applicable condition is demonstrated under the approved decision rule. FAIL means it is not met; HOLD means a decision remains unresolved; N/A means justified non-applicability. A repaired condition may later pass while the original failure remains in history. Risk acceptance shall preserve the original finding and its approved restrictions.

3.4 Security properties

Confidentiality, integrity, availability, authenticity, authorization and accountability shall be defined for actual assets and consequences. Privacy concerns the permitted treatment of information about people and is not exhausted by confidentiality. A cryptographic digest is not proof of benign origin, and encryption alone does not establish command authorization or data freshness.

Required evidence: Object identifiers, terminology, state definitions and explicit property or claim meanings.

Decision control: Records shall not merge materially different identities, properties or decisions into a misleading single status.

4 Governance, competence and retained authority

4.1 Accountable roles

Management shall assign owners for system requirements, software, safety, security, data, supply, verification, operations and release. Delegations shall state scope, limits, competence, independence and review conditions. Outsourcing shall preserve an identifiable internal owner for retained responsibilities and access to decision-essential evidence.

4.2 Independence and challenge

The degree of review independence shall follow consequences and the risk of undetected error. Authors shall not be the sole approvers of their own essential assurance conclusions where independent challenge is required. The organization shall document conflicts and provide a protected escalation route. Commercial urgency shall not override an essential technical hold.

4.3 Competence and access

Roles shall demonstrate knowledge and practical ability for the actual technology, lifecycle activity and decision. Training attendance alone shall not establish authority. Privileged technical access and decision authority shall be managed separately. Personnel changes shall trigger appropriate access removal, handover and reassessment of duties.

4.4 Integrity and reporting

Records shall preserve facts, assumptions, allegations and uncertainty distinctly. The organization shall prohibit concealment, fabricated results, retrospective approval and suppression of credible concerns. Personnel shall be able to report vulnerabilities and unsafe behavior through controlled routes without improper retaliation. Sensitive findings shall be protected while reaching owners who can act.

Required evidence: Accountability and delegation matrix, competence demonstrations, independence arrangements, access decisions and protected concern records.

Decision control: A title, account privilege or management instruction shall not confer technical authority beyond its documented scope.

5 System context, assets and consequence classification

5.1 Context and boundaries

The system owner shall define intended functions, users, operating modes, mission phases and external dependencies. The model shall include development and maintenance paths, data flows, physical access, management planes, shared infrastructure and dormant interfaces. Boundaries shall reflect actual connectivity and control, including temporary and emergency arrangements.

5.2 Asset inventory

Inventory shall identify executable and data assets, platforms, services, owners, locations, versions, interfaces, support status and recovery needs. Discovery shall be reconciled with authoritative records. Unmanaged or unreachable assets shall remain visible as uncertainty. Inventory collection on sensitive operational systems shall use an assessed method that does not compromise required behavior.

5.3 Consequence and assurance depth

Classification shall consider credible effects on people, vehicle or mission control, critical infrastructure, confidential information and operational continuity. The organization shall assign assurance activities, independence and evidence depth from those consequences. A simple numerical ranking shall not conceal a catastrophic scenario or an unknown dependency. Shared components shall inherit the strongest relevant constraints unless isolation is demonstrated.

5.4 Continuing validity

The context shall be reviewed after architecture, connection, operating-mode, user, threat, supplier or deployment changes. Assumptions about separation, trusted users and unavailable network paths shall be demonstrated where relied upon. The assurance argument shall identify who monitors each assumption and what becomes restricted if it fails.

Required evidence: Context model, asset inventory, consequence classification, assurance assignment and assumption register.

Decision control: An unexamined interface or material unknown shall not be treated as absent or harmless.

6 Integrated safety, security and threat assessment

6.1 Scenario construction

The organization shall analyze accidental faults and intentional misuse, including their interaction. Scenarios shall identify assets, threat capabilities, access conditions, vulnerable behavior, propagation and consequences. They shall include legitimate credentials used improperly, compromised suppliers, maintenance paths, stale or corrupted information and common dependencies. Assumptions and uncertainties shall be explicit.

6.2 Protective-control consequences

Proposed authentication, isolation, shutdown, rate limiting, patching and recovery controls shall be assessed for adverse operational effects. Loss of a remote identity service, a locked account or a rejected update can affect safety or mission continuity. The required behavior during loss of trust shall be defined by mode and consequence; neither universal fail-open nor universal fail-closed behavior is acceptable without analysis.

6.3 Treatment and residual exposure

Each scenario shall have preventive, detective and recovery controls with owners and verification evidence. Risk judgments shall explain exposure, consequence, control effectiveness and limitations. Numerical scoring may organize work but shall not replace a reasoned decision. Acceptance shall identify eligible authority, exact population, duration or trigger, restrictions and monitoring.

6.4 Reassessment

Threat information, findings, incidents, changes and invalid assumptions shall reopen affected scenarios and claims. The review shall trace dependencies in both directions and consider combined failures. A prior acceptance shall not automatically extend to a new mode, connection, fleet or service provider.

Required evidence: Linked hazard-threat scenarios, control rationale, verification, residual-risk decisions and reassessment history.

Decision control: Risk acceptance shall not rewrite a failed requirement as PASS or authorize an unsafe operating condition beyond the approver's actual authority.

7 Requirements, interfaces and bidirectional traceability

7.1 Requirement quality

Requirements shall state required behavior, prohibited behavior, interfaces, timing, resource limits, modes and failure responses in verifiable terms. Security and privacy properties shall identify their assets and operating conditions. Ambiguous terms such as secure, fast or resilient shall be replaced by criteria or controlled definitions. Derived requirements shall be reviewed by the responsible system authority.

7.2 Interface contracts

Interfaces shall define identity, semantics, units, ranges, freshness, ordering, error handling, authority and timing. The organization shall address malformed, missing, duplicated, conflicting and unauthorized inputs and the effect of unavailable peers. Interface ownership and change coordination shall be agreed across organizational boundaries.

7.3 Trace relationships

Traceability shall connect context, hazards and threats to requirements, architecture, implementation, verification and deployed configuration. The organization shall identify unimplemented requirements, orphan implementation and evidence without a valid target. Coverage shall use a controlled denominator and distinguish implemented, verified, failed, deferred and approved N/A items.

7.4 Change propagation

A change shall identify all affected relationships, including test data, assumptions, tools, suppliers and user documentation. Reused evidence shall retain a documented applicability argument. The organization shall demonstrate representative forward and backward trace queries and preserve historical baselines rather than overwriting them.

Required evidence: Reviewed requirements, interface agreements, complete trace matrix, gap dispositions and change-impact records.

Decision control: A high trace percentage shall not compensate for an unverified essential requirement or a misleading denominator.

8 Architecture, isolation and resilient behavior

8.1 Allocation and boundaries

Architecture shall allocate requirements to components and identify trusted computing elements, privileged paths and shared resources. Boundaries shall separate different criticalities and trust levels where necessary. The organization shall justify each crossing and identify the controls, failure behavior and evidence required to preserve isolation.

8.2 Common causes and independence

Redundancy claims shall examine shared software, data, power, clocks, identity services, development tools, administrators and update channels. Diverse labels or separate virtual machines alone do not demonstrate independence. The analysis shall address simultaneous compromise, cascading failures and resource exhaustion. Independence claims shall state their physical, logical and organizational limits.

8.3 Degraded and protective modes

The design shall define permitted behavior when inputs, communication, trust, compute resources or time references are degraded. Transitions shall preserve necessary control authority, observability and operator understanding. Recovery shall avoid oscillation, stale-command execution and unintended reactivation. Safety and security owners shall jointly resolve conflicting protection objectives.

8.4 Verification of architecture

Evidence shall demonstrate boundary enforcement and representative failure behavior, including management and maintenance paths. Architectural assumptions shall be carried into integration and deployment criteria. A diagram or approved design document alone shall not establish that the deployed boundary works.

Required evidence: Architecture and dependency models, isolation arguments, common-cause analysis, mode definitions and representative boundary evidence.

Decision control: Unproven isolation shall not justify reducing assurance of a shared or connected component.

9 Lifecycle planning, reviews and independent assurance

9.1 Integrated planning

The lifecycle plan shall define activities, owners, inputs, outputs, entry and exit criteria, independence and record control. It shall integrate safety, security, privacy, configuration, supplier and operational work. Iterative delivery is permitted when each increment preserves required evidence and authorized scope. A sprint completion or schedule milestone shall not substitute for a technical gate.

9.2 Review gates

Reviews shall examine actual baselines, unresolved findings and downstream dependencies. Required participants shall have relevant authority and competence. Decisions shall identify permitted next work, restrictions, evidence gaps and invalidation triggers. Conditional approval shall not be displayed as unrestricted release.

9.3 Verification independence

The plan shall identify where separate authorship, review, witnessing or independent verification is required. Independence shall be evaluated for access, reporting lines, incentives and ability to challenge assumptions. The responsible authority shall justify any combined roles and retain controls against self-confirming evidence.

9.4 Evidence continuity

Plans and review records shall remain synchronized with actual work and changes. Evidence shall be available for the necessary support life and recovery scenarios. When development is transferred, the receiving organization shall demonstrate the ability to build, verify, maintain and interpret the transferred baseline before relying on it.

Required evidence: Integrated lifecycle plan, review schedule, eligibility and independence records, gate decisions and evidence handover.

Decision control: A planned activity or future corrective action shall not be presented as completed assurance.

10 Suppliers, reusable software and dependency transparency

10.1 Acquisition and retained duties

Before commitment, the purchaser shall define intended use, consequence, evidence access, support obligations, vulnerability reporting, change notification and end-of-support arrangements. Supplier approval shall identify the actual product, service, site and activity. Commercial reputation or a general certificate shall not establish suitability for an aerospace function. The purchaser shall retain an owner for integration and continuing-use decisions.

10.2 Component and dependency records

The organization shall maintain an SBOM or equivalent controlled inventory tied to actual release artifacts. Records shall distinguish direct and transitive dependencies, versions, identifiers, origin, relationships, inclusion status and known limitations. Runtime-loaded components, firmware, containers, plugins and externally hosted dependencies shall be addressed where relevant. Unknown completeness shall be stated rather than represented as a complete inventory.

10.3 Suitability and vulnerability context

Reused components shall be assessed for intended environment, unsupported assumptions, known defects, licensing or usage restrictions, update mechanisms and maintenance capability. A vulnerability applicability statement shall identify the exact version, deployed configuration, reachable behavior and evidence. Absence from a scanner result shall not prove absence of a vulnerability. Reachability analysis shall consider privileged and maintenance paths.

10.4 Supplier change and continuity

Contracts and technical controls shall support timely findings exchange, retained evidence and controlled replacement. Supplier discontinuation, compromise, ownership change or inability to provide evidence shall trigger an impact review. Escrow, alternative supply or internal support arrangements shall be demonstrated where relied upon; a contractual promise alone does not establish recoverability.

Required evidence: Supplier scope and agreements, release-linked dependency inventory, suitability evaluations, vulnerability applicability and continuity evidence.

Decision control: An incomplete inventory or inaccessible essential evidence shall remain a limitation on the release claim.

11 Configuration, baseline and change control

11.1 Controlled configuration items

Configuration control shall include requirements, architecture, source, build scripts, dependencies, toolchains, tests, data, infrastructure definitions, firmware, model parameters and operational settings as applicable. Baselines shall preserve relationships and effectivity. The organization shall distinguish approved source, built artifacts, released packages and deployed instances.

11.2 Change assessment

Each proposed change shall identify purpose, origin, old and new state, affected requirements and dependent evidence. Assessment shall consider safety, security, timing, resources, privacy, compatibility, support and recovery. The authority shall decide required review and reverification before implementation. An emergency change shall retain accountable authorization, restricted scope and prompt evidence completion without fabricating retrospective approval.

11.3 Integrity and access

Repositories and artifact stores shall enforce least necessary access, protected approvals and traceable change history. Controls shall detect or prevent unauthorized modification and substitution. Branch names and tags shall not be the only identity for released content. Deleted or force-replaced history shall not erase decision-essential evidence.

11.4 Deployment reconciliation

The organization shall determine the actual installed configuration and reconcile it with approved effectivity. Mixed fleets, partial updates, local overrides and drift shall remain visible. Unknown or unsupported states shall be contained or explicitly restricted. Recovery shall restore configuration relationships and authorization history, not merely file availability.

Required evidence: Configuration plan, item inventory, baseline manifests, approved changes, integrity records and actual deployment reconciliation.

Decision control: A release identifier shall not imply that every deployed instance contains the same approved configuration.

12 Software design, implementation and code review

12.1 Design and implementation rules

The development authority shall select language, design and coding rules appropriate to consequence, execution environment and maintainability. Rules shall address memory and resource management, numeric behavior, error handling, interfaces, concurrency and unauthorized access as applicable. Exceptions shall identify rationale, verification and eligible approval. Generated and externally supplied code shall remain within the assurance scope.

12.2 Defensive behavior

Implementation shall validate inputs at relevant boundaries and enforce authorization for actual operations. Error paths shall avoid uncontrolled state, information exposure and unsafe recovery. The design shall manage allocation failures, numeric overflow, invalid conversions and stale or inconsistent data. Defaults shall support the approved operating context; undocumented maintenance bypasses and embedded production secrets shall be prohibited.

12.3 Review and analysis

Reviews shall examine requirements, design intent, failure behavior, security properties and integration assumptions. Automated findings shall be triaged with their actual tool configuration and limitations. Suppression shall retain rationale and reviewer identity. A clean static-analysis result shall not replace dynamic, architectural or system-level verification. Review scope shall include changed dependencies and generated outputs where they affect behavior.

12.4 Defects and technical debt

Defects shall identify affected configurations, consequences, evidence and disposition. Deferred work shall retain owner, restrictions and invalidation triggers. Refactoring shall preserve or re-establish required behavior and traceability. A technically convenient workaround shall not silently become the permanent product requirement.

Required evidence: Approved development rules, design records, reviewed implementation, analysis results, justified exceptions and defect dispositions.

Decision control: Compilation success or absence of tool warnings shall not establish correct, safe or secure behavior.

13 Build environments, delivery pipelines and artifact provenance

13.1 Protected build context

The organization shall define and control build workers, identities, source inputs, dependencies, network access, scripts and credentials. Untrusted contributions shall not gain access to release secrets or privileged production runners. Build caches and intermediate artifacts shall be assessed as potential substitution paths. The environment shall prevent uncontrolled dependencies from entering a release.

13.2 Provenance and reproducibility

Each release build shall retain source identity, dependency resolution, tool versions, options, environment, operator or service identity and resulting artifact digests. Reproducibility shall be defined: byte-identical results or another justified comparison with explained nondeterminism. Independent reconstruction shall be performed where required by assurance depth. Differences shall be investigated rather than concealed by relabeling.

13.3 Gate and signing control

Pipeline gates shall be protected from unauthorized alteration and shall fail visibly when required checks are missing or invalid. Signing authority shall be separated from uncontrolled development execution. Signing shall bind the approved artifact and relevant manifest under a controlled trust policy. A successful pipeline or signature shall not bypass eligible technical release approval.

13.4 Pipeline incidents and recovery

Compromise, credential exposure, unexpected input or provenance gaps shall trigger containment and an affected-artifact assessment. Recovery shall re-establish trusted sources, tools, credentials and build state. Previously issued artifacts shall be assessed for recall or restriction. Restoring a runner image alone does not prove that its outputs are trustworthy.

Required evidence: Build baseline, access and secret controls, provenance, reconstruction evidence, protected gate results and affected-artifact decisions.

Decision control: An artifact with unresolved provenance or a compromised trust path shall not receive an unrestricted release claim.

14 Tool assurance, models and formal methods

14.1 Intended-use evaluation

Tools that create, transform, verify or approve decision-essential content shall be evaluated for their intended use. The assessment shall identify plausible tool errors, whether those errors would be detected independently, consequence and required assurance. A vendor claim or prior use in another environment shall not establish suitability for the current version, options and workflow.

14.2 Demonstration and continuing control

Tool evidence shall use representative inputs, expected outputs, adverse cases and known limitations. Configuration, plugins, host environment and data formats shall be controlled. Changes shall trigger impact review and necessary reverification. Tool access shall not permit silent alteration of original results or authoritative requirements.

14.3 Models and formal arguments

A model shall identify purpose, abstraction, assumptions, boundaries and connection to the implemented system. Formal results shall identify the properties proven, assumptions, solver or method limitations and excluded behaviors. Correctness of a model does not automatically establish correctness of generated code, hardware integration or operational inputs. Translation and refinement claims shall have their own evidence.

14.4 Tool failure and fallback

The organization shall define response to erroneous output, unavailable services and lost tool support. Historical conclusions shall be traced to affected versions and re-examined where necessary. Fallback manual or alternative methods shall have demonstrated capability. A tool update shall not erase the ability to interpret earlier evidence.

Required evidence: Tool inventory, intended-use assurance decisions, validation cases, model assumptions, formal proof scope and change-impact records.

Decision control: A tool-produced approval or proof result shall be limited to its demonstrated configuration, assumptions and properties.

15 Verification and validation strategy

15.1 Planned evidence

Verification shall address whether the implementation meets specified requirements; validation shall address suitability for intended use in the stated context. The strategy shall combine reviews, analysis, simulation, testing and operationally representative demonstrations as appropriate. Each method shall have defined scope, expected outcomes, independence, environment and acceptance rules before execution.

15.2 Representative environments

Differences between test and target hardware, timing, data, permissions, networks, loads and failure modes shall be recorded and justified. Simulators and test doubles shall not conceal real interface or resource behavior. The organization shall identify which conclusions require target or integrated evidence. Representative adverse and degraded cases shall be included.

15.3 Authorized security examination

Security testing shall have an approved scope, rules, target authority, protective measures, data handling and stop conditions. Testing shall use isolated or otherwise controlled environments when operational consequences cannot be safely bounded. Findings shall identify observed behavior and impact without overstating untested exploitation paths. Test permission shall not be inferred from public connectivity.

15.4 Evidence validity

Records shall retain baseline, method, inputs, expected and actual results, instrumentation, raw evidence, deviations and reviewer. Invalid or interrupted runs shall remain visible. Repeated testing shall not discard unfavorable outcomes without explanation. Evidence reuse shall identify equivalence and limitations for the changed object.

Required evidence: Verification and validation plan, authorized security-test scope, representative environments, complete results and eligible evidence review.

Decision control: Test execution, coverage or absence of observed faults shall not by itself establish all required properties or eliminate residual uncertainty.

16 Coverage, test data and anomaly disposition

16.1 Coverage measures

Coverage shall be defined for requirements, interfaces, modes, structural elements, threat scenarios and data populations as applicable. Denominators and exclusions shall be controlled. Structural coverage shall be interpreted together with requirements-based tests; executing a branch does not demonstrate that its behavior is correct. Unreachable or deactivated code shall have a justified disposition and controlled activation assumptions.

16.2 Test-data integrity

Test data shall identify origin, selection, transformations, expected outcomes and restrictions. Synthetic or anonymized data shall be assessed for representativeness and residual privacy risks. Evaluation data shall not be silently reused for tuning in a way that invalidates independence. Data corruption, leakage and mislabeled expected results shall be considered in evidence review.

16.3 Anomalies and retest

An anomaly shall record the original observation, baseline, reproducibility, impact and uncertainty. The responsible authority shall distinguish product, requirement, environment, tool and test defects. Correction shall include affected-scope analysis and appropriate regression. A passing retest shall not erase a previously unexplained intermittent failure.

16.4 Closure and reporting

Reports shall show residual gaps, failed conditions, invalid tests and deferred actions. Coverage percentages shall be accompanied by the significance of uncovered items. A single essential unresolved condition may block release even when aggregate coverage is high. Closure shall identify evidence, authority and any remaining operating restrictions.

Required evidence: Coverage model, complete denominators, controlled data, anomaly records, regression results and bounded conclusions.

Decision control: Exclusions, data selection or repeated runs shall not be manipulated to produce a misleading passing result.

17 Timing, concurrency and resource integrity

17.1 Budgets and assumptions

The design shall specify deadlines, end-to-end latency, jitter, sampling, storage, memory, bandwidth and compute budgets where they affect required behavior. Budgets shall include interference, authentication, logging, recovery and worst relevant operating modes. Average observed execution time shall not be represented as a demonstrated worst-case bound.

17.2 Concurrency and state

Analysis and verification shall address scheduling, blocking, priorities, races, deadlocks, reentrancy and asynchronous events. Shared state and resource ownership shall be explicit. Initialization, restart and mode transitions shall preserve necessary invariants. Timeouts shall be justified for actual delays and consequences rather than selected only for convenience.

17.3 Exhaustion and interference

The organization shall examine bounded and sustained overload, malformed traffic, storage saturation and resource leaks. Partitioning and admission controls shall preserve essential functions where required. Monitoring and security agents shall be included in resource and timing assessments. A protective action shall not create an unexamined priority inversion or starvation condition.

17.4 Evidence and margins

Timing and capacity evidence shall identify measurement uncertainty, platform configuration, workload coverage and analytical assumptions. Margins shall be approved for actual consequence and variability. Changes in compiler, processor, workload, cryptography or virtualization shall reopen affected budgets. Unmeasured headroom shall not be assumed available.

Required evidence: Approved budgets, scheduling and interference analysis, representative stress evidence, uncertainty and change-impact decisions.

Decision control: Passing average performance or a nominal-load benchmark shall not establish deadline satisfaction under the required worst relevant conditions.

18 Identity, authentication and privileged access

18.1 Identity lifecycle

Human, device, service and workload identities shall have accountable owners, issuance rules and termination conditions. Authentication strength shall follow consequence, exposure and operational constraints. Shared or emergency identities shall have specifically justified controls and traceable use. Identity proofing, authentication and authorization shall remain separate decisions.

18.2 Authorization and privilege

Access shall be limited to required objects, actions, environments and time. Privileged and remote actions shall have enhanced controls, review and logging. Service accounts shall not inherit unnecessary interactive or administrative rights. Role changes, supplier departure and lost devices shall trigger timely reassessment and revocation.

18.3 Offline and emergency operation

The design shall define behavior when identity services, clocks or networks are unavailable. Cached credentials and emergency access shall have bounded scope, freshness, local protection and reconciliation. Emergency access shall preserve necessary safety while preventing an uncontrolled permanent bypass. Recovery shall account for actions performed during disconnection.

18.4 Review and evidence

Access reviews shall reconcile actual privileges with approved duties and detect dormant, orphaned or conflicting permissions. Authentication failures and suspicious privileged activity shall feed incident assessment. Tests shall demonstrate prohibited actions and revoked access, including alternate paths and local maintenance interfaces.

Required evidence: Identity inventory, access matrix, authentication policy, privilege reviews, emergency-use records and negative authorization tests.

Decision control: Successful authentication shall not authorize every operation or establish that the authenticated party's current intent is safe.

19 Cryptography, key lifecycle and trust services

19.1 Approved cryptographic profile

The organization shall approve algorithms, parameters, protocols, implementation constraints and trust anchors for the intended protection period and environment. Selection shall consider interoperability, performance, physical exposure and migration needs. No universal algorithm or key size is assigned by this standard. Proprietary encoding or an unauthenticated checksum shall not be represented as cryptographic protection.

19.2 Keys and secrets

Generation, provisioning, storage, use, rotation, backup, recovery, revocation and destruction shall have accountable control. Private keys and secrets shall not be placed in ordinary source, logs or broadly accessible images. Access and separation of duties shall follow consequence. Nonces, counters and entropy sources shall be evaluated for their actual security function, including restart and rollback behavior.

19.3 Trust and compromise

Verification shall assess authenticity, permitted signer, validity conditions, revocation and intended target as applicable. An expired or compromised credential shall trigger a bounded assessment of affected artifacts, sessions and historical evidence. Offline revocation handling shall be designed rather than assumed immediate. Key recovery shall not create a route to unauthorized signing or decryption.

19.4 Agility and transition

The organization shall inventory cryptographic dependencies and assess future migration, including long-lived confidentiality and signature verification. A transition shall preserve compatibility, boot and update recoverability, evidence authenticity and timing margins. Dual algorithms or new libraries shall be verified as a changed system; migration labels alone do not establish increased assurance.

Required evidence: Approved crypto profile, key and trust inventory, protected lifecycle records, compromise response and migration evidence.

Decision control: A valid signature or encrypted channel shall not substitute for target authorization, data freshness, compatible configuration or verified content behavior.

20 Data integrity, privacy and information handling

20.1 Data purpose and ownership

The organization shall identify data owners, intended purposes, authoritative sources, quality criteria, sensitivity, users and retention needs. Flight, mission, engineering, maintenance, personal and security data shall be treated according to actual consequence. Collection shall be limited to justified purposes and applicable obligations. A technical ability to collect data shall not imply permission to use or disclose it.

20.2 Integrity and transformation

Data pipelines shall preserve identity, units, ordering, provenance and transformation history. Validation shall detect unacceptable missing, stale, duplicated, inconsistent or corrupted values. Approved substitution, interpolation or defaulting shall remain visible. The consumer shall know the quality and age needed for its decision; successful transport does not establish semantic correctness.

20.3 Privacy and controlled disclosure

Access, transfer, sharing and retention shall reflect purpose and applicable rights or restrictions. Test, diagnostic and incident records shall avoid unnecessary sensitive content. De-identification shall be assessed against actual re-identification risks. Requests to access, correct, restrict or remove personal data shall be handled through an accountable process while preserving legitimate safety and evidence duties.

20.4 Retention and recovery

Retention and disposal shall identify exact scope, authority, dependencies and legal or investigative holds. Recovery shall preserve semantics, links, configuration and access control. Corrupted or uncertain data shall not be silently restored to authoritative status. Historical decision evidence shall remain interpretable through migrations.

Required evidence: Data inventory, purpose and access rules, quality and transformation checks, privacy decisions and verified retention or recovery records.

Decision control: Possession, encryption or anonymization of data shall not by itself establish permitted use or fitness for a safety-relevant decision.

21 Communications, interfaces and distributed-system behavior

21.1 Communication contract

Each interface shall define peers, identity, authority, message semantics, permitted direction, freshness, timing and failure response. Protection shall address integrity, confidentiality and availability according to consequence. Network location alone shall not establish trust. Management, diagnostic, payload and safety-related communication paths shall be identified separately.

21.2 Freshness and distributed state

The design shall address delay, reordering, replay, duplication, loss, partition and reconnection. Sequence numbers, timestamps or other freshness mechanisms shall have defined wrap, reset, persistence and clock assumptions. Commands shall not be executed merely because they arrive after reconnection. Distributed authority shall prevent conflicting controllers from issuing uncontrolled simultaneous actions.

21.3 Boundary controls and capacity

Gateways and protocols shall enforce approved operations and reject invalid inputs without unsafe resource consumption. Rate limits, filtering and inspection shall be assessed for operational effects. Encryption termination, proxying and protocol translation shall preserve the required end-to-end properties or identify their limits. Connection diagrams shall include alternate and maintenance routes.

21.4 Verification and monitoring

Tests shall include legitimate and prohibited flows, stale messages, loss of time, partial failure and recovery. Actual deployments shall be checked against the approved communication model. New peers, protocol versions, routing or remote-access paths shall trigger impact review. A successful connectivity test shall not establish the security or correctness of exchanged commands.

Required evidence: Interface contracts, flow inventory, freshness and authority model, negative-path tests and actual-network reconciliation.

Decision control: Unknown message origin, authority, freshness or interpretation shall trigger the defined protective behavior rather than an assumed valid command.

22 Platform, firmware and hardware-rooted trust

22.1 Platform baseline

The organization shall identify processors, programmable devices, boot components, firmware, drivers, operating systems and configuration relevant to assurance. Hardware debug paths, service modes and physical access shall be included. The approved platform shall identify supported combinations and known limitations; a software-only version list shall not be treated as the complete executable environment.

22.2 Boot and execution integrity

The design shall establish the required chain of trust from initial execution to loaded components. Verification shall identify permitted signers, target compatibility, rollback policy and recovery behavior. Measured-state records shall be interpreted against a trusted reference and freshness basis. Attestation shall not claim properties that the measurement cannot observe.

22.3 Isolation and physical conditions

Memory protection, privilege separation, device access and shared buses shall be assessed for the actual architecture. Physical compromise, environmental upset and persistent-state corruption shall be considered where credible. Debug interfaces shall be controlled for development, production, maintenance and retirement. Hardware features shall not be assumed enabled merely because the device supports them.

22.4 Change and recovery

Firmware, microcode, board, boot-key or platform changes shall trigger compatibility and assurance review. Recovery shall use a trusted and compatible path and avoid uncontrolled fallback to vulnerable versions. The organization shall retain a means to identify affected units and actual platform state after repair or replacement.

Required evidence: Platform inventory, boot and trust design, configured isolation evidence, debug controls and verified recovery or change records.

Decision control: Authentic boot content shall not establish correct application behavior or approval of an unsupported hardware-software combination.

23 Cloud services, virtualization and shared infrastructure

23.1 Responsibility and service boundaries

The organization shall define responsibilities for platform, application, identity, configuration, logging, keys, backup and incident response across providers and users. It shall assess actual service locations, administrative access, subcontractors and dependency changes where relevant. A provider's general assurance statement shall not establish correctness of the customer's configuration or application.

23.2 Isolation and management planes

Tenant, workload, container and virtual-machine boundaries shall be evaluated for consequence and shared-resource effects. Administrative control planes, orchestration, images and secrets shall receive explicit protection. An isolated application network shall not conceal a shared privileged management route. Templates shall be validated before broad deployment.

23.3 Availability and exit

Architecture shall address loss of regions, accounts, identity services, connectivity, quotas and provider support. Recovery and exit arrangements shall preserve data meaning, keys, provenance and operational authority. Availability promises shall be reconciled with the actual mission or service need. Provider independence shall be assessed for common infrastructure and control dependencies.

23.4 Continuous configuration assurance

Actual infrastructure shall be compared with approved definitions. Drift, unused exposure and excessive permissions shall be corrected through controlled change. Service updates outside the organization's direct control shall have monitoring and impact arrangements. Testing shall include denied actions, boundary crossings and restoration of an independently usable service.

Required evidence: Shared-responsibility matrix, configured architecture, provider dependencies, drift evidence, recovery and exit demonstrations.

Decision control: A contractual uptime target or deployment template shall not establish demonstrated resilience of the complete service.

24 Industrial, test and maintenance digital environments

24.1 Operational context

Manufacturing, test, ground-support and maintenance systems shall identify their effects on product conformity, equipment, people and evidence. Inventory shall include controllers, engineering workstations, test scripts, calibration data, removable media and remote service paths. Security controls shall be assessed against deterministic operation, legacy constraints and maintenance windows.

24.2 Segregation and access

Operational zones and conduits shall preserve necessary separation from enterprise, supplier and external networks. Remote access shall be explicitly authorized, bounded, monitored and removable. Shared engineering credentials and unmanaged maintenance laptops shall not bypass controls. Temporary connections shall be recorded and removed or incorporated into the approved baseline.

24.3 Production and test integrity

Programs, recipes, parameters and test results shall be protected against unauthorized or mistaken change. The system shall bind results to actual article, configuration, tool, method and operator. A compromised measurement or test system shall trigger an affected-product and evidence assessment. Restoring network availability alone shall not restore product-release confidence.

24.4 Safe maintenance and recovery

Patching, scanning, monitoring agents and recovery actions shall be assessed for process effects before use. Fallback and restart shall establish physical equipment state as well as digital configuration. The organization shall reconcile work in progress, interrupted tests and released records after an incident.

Required evidence: Operational inventory, zone and access model, protected program/result records, assessed maintenance and product-aware recovery evidence.

Decision control: Enterprise-security practice shall not be applied blindly where it can disrupt an essential physical or verification function.

25 Airborne and aviation ground-system integration

25.1 Integrated scope

The integrator shall identify airborne functions, connected ground services, maintenance equipment, crew interfaces and data-loading paths. Requirements shall reflect flight phases, dispatch conditions, environmental assumptions and operating permissions. A ground-service or component approval shall not be extended automatically to the integrated aircraft function.

25.2 Connectivity and control authority

Cabin, passenger, payload, maintenance and control domains shall have justified separation and permitted exchanges. Remote services shall not gain operational authority beyond the approved design. Data loading shall establish target identity, compatibility and completeness. Loss or compromise of external services shall lead to defined and verified behavior.

25.3 Operational changes and human interaction

Updates, credential expiry, diagnostics and protective actions shall be assessed for their effect on crew workload and continued operation. The interface shall communicate relevant degraded states, limitations and required actions without relying on ambiguous alerts. The operator's authority and procedures shall be reconciled with technical protection mechanisms.

25.4 Continuing assurance

Fleet configuration, known vulnerabilities, incidents and maintenance actions shall be traceable to affected installations. The organization shall define when a finding changes operating restrictions or requires new verification. Security evidence shall be integrated with the applicable system safety and operational approval processes without claiming that one replaces the other.

Required evidence: Aircraft-ground interface scope, phase-specific behavior, separation and data-load evidence, operator arrangements and fleet impact records.

Decision control: An enterprise vulnerability rating or remote update success shall not alone determine an aircraft's permitted operating state.

26 Space, remote mission and intermittent-link systems

26.1 Mission and segment model

The organization shall model spacecraft or remote platform, ground control, payload services, relay networks, suppliers and operator interfaces. The model shall include long communication delays, contact windows, limited resources, physical inaccessibility and mission phases where relevant. Trust and authority shall be explicit across every command and data path.

26.2 Command integrity and autonomy

Commands shall be authenticated, authorized, targeted and assessed for freshness, sequencing and permitted state. Autonomous behavior shall remain within approved constraints and identify intervention or fallback conditions. Lost links, stale mission plans, competing ground stations and corrupted time or position sources shall have defined responses. Physical inaccessibility shall not justify unexamined permanent trust assumptions.

26.3 Update and recovery feasibility

Update plans shall account for contact capacity, power, storage, verification, interruption and recoverable execution paths. The organization shall distinguish an available image from a technically safe opportunity to activate it. Key rotation and revocation shall address disconnected assets and long mission life. A recovery route shall be demonstrated before it is relied upon for irreversible deployment.

26.4 Mission continuity and evidence

Operations shall retain command provenance, acknowledgments, observed state and uncertainty. Missing telemetry shall not be interpreted as proof of successful execution. Ground-segment recovery shall reconcile authority, pending commands and spacecraft state before resuming control. Threat and fault assessments shall include shared ground-service dependencies.

Required evidence: Segment and authority model, command-state rules, contact-aware update plan, autonomous constraints and mission recovery demonstrations.

Decision control: Loss of contact or delayed acknowledgment shall not authorize unsafe repeated commands or a claim of confirmed remote state.

27 Machine learning, trained models and adaptive functions

27.1 Intended use and operational boundary

The model owner shall define intended decisions, prohibited uses, operating domain, consequences and human or technical supervision. The assurance argument shall identify why the selected model is suitable and where deterministic controls are required. A generic accuracy claim shall not establish suitability for a safety-related aerospace function.

27.2 Data and model provenance

Training, validation and evaluation data shall identify origin, permissions, labeling, transformations, exclusions and population coverage. Splits shall avoid leakage across correlated entities or time periods. The model baseline shall include architecture, weights, preprocessing, thresholds, dependencies and training configuration. External models shall have sufficient evidence for the actual intended use or explicit restrictions.

27.3 Evaluation and safeguards

Evaluation shall examine important subpopulations, rare consequential conditions, distribution shift, uncertainty and adversarial or corrupted inputs as relevant. Metrics shall state denominators and uncertainty. Safeguards shall detect or bound out-of-domain behavior and provide a verified fallback. A human-in-the-loop claim shall demonstrate that the person has information, time, competence and real ability to intervene.

27.4 Change and operation

Model, data, threshold and preprocessing changes shall follow controlled impact assessment and reevaluation. Online adaptation shall be bounded and monitored under an approved assurance strategy; unrestricted learning shall not silently alter accepted behavior. Drift and adverse events shall trigger defined restrictions and retraining or retirement decisions.

Required evidence: Model-use specification, data and training provenance, independent evaluation, safeguard evidence, deployed model identity and drift controls.

Decision control: Aggregate model performance or a provider's model card shall not compensate for an unresolved essential scenario or unsupported operating domain.

28 AI-assisted development and agentic tools

28.1 Authorized assistance

The organization shall define permitted uses of generative or agentic tools in requirements, code, testing, analysis and operations. It shall classify outputs by consequence and specify review and verification. Generated content shall be treated as unverified until the required evidence exists. Tool use shall not transfer technical accountability to the model or provider.

28.2 Data and instruction boundaries

Prompts, retrieved material and tool outputs shall be assessed for sensitive-data exposure, provenance and malicious or misleading instructions. Access to repositories, credentials, deployment and operational systems shall be limited to the approved task. Untrusted content shall not acquire authority to override controlled instructions or grant permissions.

28.3 Review and independent evidence

Review shall assess correctness, security, rights of use, assumptions and traceability. AI-generated tests shall not be the sole evidence for AI-generated implementation where common errors can escape both. Critical conclusions shall be checked against authoritative requirements and independent observations. Plausible explanations and fabricated citations shall not be accepted as evidence.

28.4 Autonomous actions and recovery

Agentic workflows shall define action limits, approval points, transaction boundaries, logging, interruption and rollback. Consequential operations shall require the eligible human or system authority specified in the approved workflow. The organization shall test prohibited actions and recovery from partial execution. A task-success message shall be reconciled with actual resulting state.

Required evidence: Approved use cases, data and access boundaries, review records, independent verification and agent-action containment evidence.

Decision control: Generated output, confidence language or apparent task completion shall not constitute technical approval or permission for an unbounded autonomous action.

29 Hardening, secure configuration and deployment readiness

29.1 Approved deployment profile

The deployment authority shall define permitted services, ports, accounts, privileges, security settings, logging, data paths and supported configurations. Unnecessary functions shall be disabled or justified. Defaults shall be reviewed for the actual context. The profile shall distinguish development, test, maintenance and operational states and control transitions between them.

29.2 Readiness and target identity

Before installation, the organization shall verify target identity, configuration, prerequisites, capacity, permissions, recovery route and approved artifact. The readiness record shall identify affected users and operational windows. A technically valid package shall not be installed on an incompatible target or during an unauthorized operating condition.

29.3 Commissioning and drift

Commissioning shall verify actual behavior, access restrictions, interfaces, monitoring and fallback. Automated configuration shall be checked against resulting state. Drift shall be detected, assessed and corrected through controlled change. Local exceptions shall identify owner, reason, evidence, limitations and expiry or review triggers.

29.4 Handover

Operations shall receive the exact baseline, known limitations, support contacts, incident routes, recovery procedures and required training. The receiving owner shall confirm ability to operate and maintain the system. Unresolved dependencies shall remain visible with blocked scope rather than disappearing at project handover.

Required evidence: Deployment profile, readiness and target checks, commissioning results, drift records and accepted operational handover.

Decision control: Installation success or service availability shall not by itself establish secure configuration or permission for unrestricted operation.

30 Updates, offline delivery and rollback control

30.1 Update package and authority

The update dossier shall identify source and target baselines, changed components, dependencies, prerequisites, known issues, verification and eligible approval. Delivery shall protect package integrity and authenticity and bind installation to permitted targets. A signature shall not replace compatibility, release or operating-state checks. Offline media shall preserve the same necessary controls.

30.2 Activation and interruption

The update design shall distinguish transfer, validation, installation, activation and confirmation. It shall define behavior for lost power, interrupted links, incomplete data, storage exhaustion and mixed-version states. Activation shall occur only in approved conditions. The organization shall demonstrate that interrupted execution does not produce an unexamined unsafe or irrecoverable state.

30.3 Rollback and anti-rollback

Rollback policy shall reconcile recovery needs with protection against vulnerable or incompatible versions. Approved recovery images shall have known limitations and target applicability. Monotonic counters, state schemas and trust changes shall be assessed for their effect on recovery. A data migration may make binary rollback insufficient; the complete state transition shall be verified.

30.4 Fleet rollout and confirmation

Staged deployment shall use justified populations, observation criteria and stop or expansion rules. Actual installed state and failed or unreachable targets shall be reconciled. A package-delivery acknowledgment shall not be treated as confirmation of activation or correct behavior. Urgent security updates shall retain safety, compatibility and authorization gates.

Required evidence: Update dossier, package provenance, target rules, interruption and recovery tests, rollout decisions and actual fleet-state records.

Decision control: Urgency shall not authorize an unverified update path or hide partially updated or unreconciled assets.

31 Logging, detection and operational monitoring

31.1 Monitoring objectives

Monitoring shall identify the conditions to detect, relevant assets, consequence, required response and evidence sources. Coverage shall include privileged actions, trust changes, configuration drift, failed controls and operational anomalies as appropriate. Logging volume alone shall not be represented as effective detection. Blind spots and unavailable sources shall be visible.

31.2 Event integrity and time

Records shall preserve source identity, event meaning, relevant baseline, time basis and uncertainty. Clock loss, skew, wrap and resynchronization shall be handled explicitly. Collection and storage shall resist unauthorized alteration and loss. Secrets and unnecessary personal information shall be excluded. Correlation shall not imply an exact event order beyond available time accuracy.

31.3 Detection validation

Detection rules and models shall be evaluated using representative legitimate and adverse cases. The organization shall measure relevant missed detections, false alarms, workload and response performance with clear denominators. Threshold changes shall be controlled. A higher alert count shall not automatically be interpreted as a worse security posture or a better detector.

31.4 Response and capacity

Alerts shall have accountable owners, escalation criteria and operationally feasible actions. Storage, communication and processing capacity shall support required retention and detection under relevant loads. Loss of monitoring shall trigger defined restrictions or alternate arrangements. Automated responses shall remain within approved safety and authority bounds.

Required evidence: Monitoring plan, event schema, time-quality evidence, detector validation, response routes and blind-spot or capacity records.

Decision control: Silence, missing logs or a green dashboard shall not establish absence of compromise or valid operation.

32 Vulnerability intake, applicability and remediation

32.1 Intake and coordination

The organization shall maintain accessible reporting and trusted information routes for product and infrastructure vulnerabilities. Reports shall be acknowledged, protected and assigned for assessment. Triage shall preserve the reported facts and avoid exposing sensitive details unnecessarily. Supplier and operator coordination shall identify who assesses, decides, communicates and acts.

32.2 Applicability and priority

Assessment shall identify affected versions, configurations, paths, privileges, exposure and consequences. Priority shall consider actual safety or mission effects, exploitation evidence, controls, support state and uncertainty. A generic severity score shall inform rather than replace the decision. Unverified non-applicability shall remain unresolved.

32.3 Treatment and deadlines

The eligible authority shall select correction, mitigation, restriction, withdrawal or justified temporary acceptance. Deadlines shall follow risk and actual feasibility, with interim controls and review triggers. A deferred patch shall identify the affected population and residual exposure. Exceptions shall not renew indefinitely without fresh evidence and authority.

32.4 Verified closure

Remediation shall follow controlled change, regression, deployment and fleet reconciliation. Closure shall demonstrate that the intended population is corrected or remains explicitly restricted. Publication of an advisory or availability of a patch alone shall not establish implementation. Recurrence shall feed causal analysis and development improvements.

Required evidence: Intake records, configuration-specific applicability, priority rationale, treatment decisions, communications and verified population closure.

Decision control: A scanner status or patch release shall not close an unresolved vulnerability on an unverified deployed target.

33 Incident response, evidence preservation and communication

33.1 Preparation and authority

Incident plans shall define triggers, roles, protected contacts, technical authority, communications and relationships to safety and mission control. Exercises shall include unavailable identity or communication services and cross-supplier dependencies. Responders shall know which actions they may take and which require operational coordination.

33.2 Detection, assessment and containment

The response shall preserve known facts, uncertainty, time basis and affected scope. Containment shall account for physical and mission consequences; indiscriminate shutdown or network isolation shall not be assumed safe. The responsible authority shall select proportionate actions and record why continued, restricted or stopped operation is permitted.

33.3 Evidence and notification

Evidence collection shall preserve provenance, integrity, access history and handling constraints. Live collection shall be assessed for its effect on systems and volatile data. Notifications shall distinguish confirmed facts from hypotheses and state immediate protective actions and update conditions. Applicable notification obligations and recipient needs shall be identified locally; this standard assigns no universal notification deadline.

33.4 Eradication, recovery and lessons

Recovery shall address persistence, compromised identities, trust anchors, data and affected releases. Restart shall require an eligible decision based on verified state and residual restrictions. The organization shall reconcile potentially affected products, commands and records. Lessons shall lead to verified corrective action and updated scenarios, not only a narrative incident report.

Required evidence: Incident plan, exercises, chronology, containment rationale, preserved evidence, notifications and authorized recovery or corrective action.

Decision control: Service restoration shall not be equated with incident closure or restored trust in all historical outputs.

34 Backup, recovery and operational continuity

34.1 Recovery requirements

The organization shall define recovery-time and recovery-point objectives, permitted degraded states, minimum functions and data-consistency needs. Objectives shall reflect actual consequence and dependencies. The plan shall identify identity, keys, licenses, tooling, suppliers and human resources needed for restoration. Backup frequency alone shall not establish the recoverable state.

34.2 Protected recovery assets

Backup and recovery copies shall be protected from the same credible compromise paths that affect production where necessary. Retention, isolation, access, integrity and restoration compatibility shall be controlled. A copy that cannot be decrypted, interpreted or restored with available dependencies shall not count as a usable recovery capability.

34.3 Demonstrated restoration

Exercises shall restore representative complete services and data relationships, including authorization and configuration. Measured recovery time shall include detection or declaration boundaries as defined, restoration, validation and return-to-service decisions. Tests shall examine corrupted, unavailable and stale copies. A successful file restore shall not establish semantic or operational recovery.

34.4 Reconciliation and continuity

After recovery, pending transactions, commands, product results and externally issued decisions shall be reconciled. The organization shall prevent duplicate actions and silent loss. Continuity arrangements shall be reviewed after architecture, capacity, threat and support changes. Residual gaps shall remain visible in operational restrictions.

Required evidence: Recovery objectives, dependency map, protected backup records, representative restoration results and reconciled return-to-service decisions.

Decision control: An untested backup or provider promise shall not establish achieved recovery objectives.

35 Human interfaces, remote support and operational competence

35.1 Human-system interaction

Interfaces shall communicate modes, authority, degraded states, warnings and required action consistently. Design and evaluation shall consider workload, ambiguity, alert overload and foreseeable error. Security tasks shall be operationally feasible. A human safeguard shall have demonstrated information, time and capability to act under relevant conditions.

35.2 Remote and maintenance support

Remote sessions shall identify purpose, target, operator, permitted actions and duration. Access shall be approved, protected, monitored and terminated when no longer required. File transfer and privileged actions shall be controlled. The owner shall reconcile resulting configuration and operational state. Supplier availability shall not justify permanent unrestricted access.

35.3 Training and exercises

Training shall cover actual roles, failure scenarios, reporting, protective actions and handover. Competence shall be demonstrated through practical evidence appropriate to consequence. Exercises shall include conflicting information, unavailable services and limits of automation. Operators shall know when to escalate rather than improvise an unsafe bypass.

35.4 Handover and fatigue-sensitive work

Shift and organizational handovers shall preserve active incidents, exceptions, pending changes, remote sessions and blocked decisions. Critical work shall account for workload and conditions that impair reliable action. The organization shall assign independent checks where consequence requires them and retain accountability for shared tasks.

Required evidence: Human-interface evaluation, remote-session records, role competence, exercises and complete operational handovers.

Decision control: Training attendance or the nominal presence of a human shall not establish an effective human control.

36 Assurance case, release and truthful claims

36.1 Structured assurance argument

The release authority shall assemble a coherent argument connecting scope, consequences, requirements, design, implementation, evidence and residual limitations. Claims shall identify the exact artifact, platform, configuration, environment and intended use. Evidence shall be current and applicable, with assumptions and contradictions explicitly resolved or retained as restrictions.

36.2 Release prerequisites

Release shall require reconciled baselines, valid verification, reviewed findings, dependency transparency, approved risk decisions, deployment readiness and support arrangements as applicable. The authority shall verify completeness rather than rely solely on a checklist score. Essential unresolved FAIL or HOLD conditions shall block the affected scope unless an explicitly permitted bounded departure has valid authority and does not falsely assert conformity.

36.3 Declaration and operational handoff

The release statement shall identify issuer, authority, object, version or digest, target scope, evidence basis, restrictions and effective conditions. Operational authorization shall identify the actual installation and permitted modes. Statements shall not imply immunity from cyberattack, defect-free software or permission beyond the evidence.

36.4 Amendment and withdrawal

New findings, compromised provenance or invalid assumptions shall trigger assessment of issued claims and affected users. Corrections, restrictions and withdrawal shall preserve the original record and notification history. A changed release shall not silently replace historical evidence used for prior operations.

Required evidence: Assurance case, complete release dossier, authenticated decision, deployment handoff and amendment or withdrawal history.

Decision control: Release shall remain bounded by demonstrated evidence and eligible authority; no aggregate metric shall conceal an unresolved essential condition.

37 Legacy systems, obsolescence and continuing support

37.1 Legacy baseline

The organization shall reconstruct the actual configuration, interfaces, operational dependencies and available evidence for legacy systems. Unknown source, unsupported components and undocumented access paths shall remain explicit. Continued past operation shall not be the sole argument for present safety or security under changed exposure.

37.2 Compensating controls

Where immediate correction is infeasible, compensating controls shall identify the scenario addressed, demonstrated effectiveness, limitations, owner and review triggers. Isolation, monitoring or restricted use shall be verified against actual alternate paths. A compensating control shall not be claimed to correct unrelated defects or remove a required technical property.

37.3 Support and transition

The support plan shall cover expertise, tools, keys, spare platforms, source access, vulnerability handling and recovery capability. Migration shall assess data meaning, timing, interfaces, operator behavior and retained evidence. Replacement shall use staged, verified transition with rollback or another justified recovery route.

37.4 Continued-use decisions

Continued use shall be periodically and event-trigger reviewed against current threats, consequence and available controls. The organization shall identify conditions requiring restriction, replacement or withdrawal. Commercial cost and schedule shall be explicit constraints, not concealed reasons for weakening evidence or redefining the requirement.

Required evidence: Legacy baseline and gaps, demonstrated compensating controls, support plan, migration evidence and bounded continued-use decisions.

Decision control: End-of-support acceptance shall not imply that unsupported software remains adequately protected without a demonstrated and maintained argument.

38 Retirement, transfer and secure disposal

38.1 Retirement plan

Retirement shall identify assets, dependencies, owners, data, credentials, interfaces and outstanding obligations. The organization shall assess effects on systems that still rely on the retiring service, trust anchor or record store. Withdrawal shall include users, suppliers and recovery arrangements where relevant.

38.2 Access and trust termination

Accounts, device identities, certificates, remote access, routes and integration credentials shall be removed or revoked through controlled action. The organization shall verify that the retired asset cannot retain unintended authority. Shared credentials and keys shall be assessed for replacement on continuing systems. Physical transfer shall not imply transfer of digital authority.

38.3 Data and evidence disposition

Data shall be retained, transferred, sanitized or destroyed according to approved purpose and obligations. Sanitization shall be appropriate to the medium and sensitivity and verified by a justified method. Evidence needed for product history, investigations or continuing claims shall remain accessible. Disposal records shall not expose the secrets they document.

38.4 Closure and residual dependencies

The owner shall reconcile inventory, contracts, backups, logs, DNS or equivalent naming, subscriptions and external access. Orphaned resources shall be assessed for exposure and unauthorized reuse. A transfer shall define custody, permitted use and remaining duties. Closure shall identify any retained records, keys or services and their accountable owners.

Required evidence: Retirement plan, dependency review, verified authority removal, data disposition and reconciled closure record.

Decision control: Physical removal or subscription cancellation alone shall not establish secure retirement.

39 Assurance reviews, metrics and evidence continuity

39.1 Risk-based examination

Assurance shall examine representative end-to-end trails from requirement to deployed behavior and from an incident or artifact back to source evidence. Selection shall include critical functions, suppliers, abnormal cases and failed controls. Document presence shall not establish effective implementation. Reviewers shall have competence and independence appropriate to consequence.

39.2 Findings and corrective action

Findings shall state requirement, actual evidence, affected scope, consequence and uncertainty. Closure shall verify implemented correction and effectiveness. The eligible closure authority shall be sufficiently independent of the corrective work. A favorable overall assessment shall not neutralize an unresolved essential finding.

39.3 Metrics and management decisions

Metrics shall define populations, time windows, denominators and limitations. Management shall review vulnerability exposure, assurance gaps, incidents, change failures, recovery evidence, support risks and resource adequacy. Mean values shall not hide severe tails or critical subpopulations. Decisions shall allocate owners and resources and preserve necessary restrictions.

39.4 Records and recovery

Retention shall reflect product life, obligations, claims and investigation needs. Migration and recovery shall preserve content, relationships, timestamps with uncertainty, configuration and decisions. Access and authentication shall support reliable attribution. Loss of essential evidence shall trigger an impact assessment on dependent releases and operations.

Required evidence: Assurance plan, representative trails, independent findings closure, interpretable metrics, management actions and verified record continuity.

Decision control: Audit completion, dashboard status or restored files shall not be represented as product acceptance or complete evidence recovery.

40 Publication, local adoption and maintenance

40.1 Publication authority

Aerospace Federation controls the publication identity, edition and authorized interpretation. Eligible publication approval shall be recorded separately from drafting and formatting. The dossier shall retain technical review, consultation, comment dispositions, consistency checks, claimed validation evidence and unresolved limitations. No document shall invent an approval, signature or effective date.

40.2 Local adoption

The adopter shall identify scope, accountable roles, applicable clauses, completed parameters, technical profiles, local methods, competence and transition. It shall identify the exact edition and controlled supporting documents. Local adoption shall not imply AF certification or recognition. Implementation shall be demonstrated through actual lifecycle and operational evidence.

40.3 Interpretation and change

Questions shall identify the requirement, actual scenario, competing readings and affected decisions. The responsible authority shall preserve the reasoned response. Informal guidance shall not silently amend normative text. Changes shall include rationale, technical review, affected requirements and transition needs. Adopters shall assess implications for existing claims and configurations.

40.4 Set coherence

Document codes, titles, source anchors and relationships shall remain consistent. Superseded conditions shall not persist in forms or digital rules without an explicit transition basis. Master lists and coverage matrices provide navigation and do not establish conformity. Historical editions, interpretations and decisions shall remain traceable where required.

Required evidence: Publication dossier, local adoption record, controlled edition, interpretation history and maintained document relationships.

Decision control: This review manuscript shall not be described as an approved publication or verified organizational implementation until the corresponding authorized decision exists.

Annex A - Activity-based applicability and retained duties

Status: Normative within the proposed AF 9500 requirement set.

A.1 Selection method

The scope owner shall identify actual activities, products, services, sites, operating modes and outsourced functions. It shall select the relevant clauses below and evaluate other clauses where their conditions exist. Shared governance, evidence and change duties shall remain applicable to every retained responsibility.

Table A-1. Activity triggers and primary clauses

Activity or responsibility	Primary clauses	Boundary to retain
Software producer	4-17, 28-30, 32-40	Intended-use evidence and release identity.
Component or service supplier	5-16, 20-23, 32-40	Exact supplied scope and limitations.
System integrator	4-17, 21-30, 35-40	End-to-end behavior and shared dependencies.
Airborne or aviation ground system	5-22, 25, 29-40	Flight-phase effects and operating authority.
Space or remote mission system	5-22, 26, 29-40	Delayed links, command state and recovery.
Industrial, test or maintenance system	4-24, 29-40	Physical and product-evidence consequences.
Cloud or shared-service operator	4-11, 18-23, 29-40	Configured responsibility and service exit.
AI or trained-model provider	4-16, 20, 27-40	Data, model and operating-domain evidence.
AI-assisted development or agents	4-16, 18-20, 28, 36-40	Untrusted output and bounded actions.
Security or verification provider	4-9, 14-16, 20, 31-40	Authorized scope and valid evidence.
Operator, maintainer or asset owner	4-11, 18-26, 29-40	Actual configuration and continuing use.

A.2 Responsibility closure

A responsibility matrix shall identify who specifies, develops, supplies, integrates, verifies, accepts, deploys, operates, maintains and retires each object. The parties shall agree evidence access, change, incident and recovery interfaces. Unassigned responsibilities shall remain open dependencies; a contract shall not silently transfer a duty that the receiving party cannot perform.

A.3 Non-applicability and reassessment

N/A decisions shall state absent conditions, evidence, authority and review triggers. A change in connection, criticality, operating mode or retained responsibility shall reopen the relevant selection. A blank template or missing capability shall not establish N/A.

Annex B - Mandatory parameter baseline and common record payload

Status: Normative within the proposed AF 9500 requirement set.

B.1 Parameter schedule

Each parameter shall have an approved value, controlled reference or justified N/A decision before dependent work. Entries shall identify scope, owner, authority, source, effectivity, units where relevant and change triggers. Values may be structured specifications or decision rules. This table assigns no universal technical level or interval.

Table B-1. P01-P44 parameter schedule

ID	Parameter	Required distinction or basis
P01	Scope and lifecycle	Objects, sites, activities and retained duties.
P02	Context and modes	Intended use, environment and dependencies.
P03	Requirement precedence	Obligations, conflicts and eligible resolution.
P04	Consequence classification	Safety, mission, information and continuity effects.
P05	Assurance depth	Methods, independence and evidence strength.
P06	Risk acceptance	Eligible authorities, restrictions and review triggers.
P07	Asset identity	Source, artifact, platform and deployed instance.
P08	Requirement and trace rules	Baselines, denominators and gap treatment.
P09	Architecture boundaries	Trust, criticality, shared resources and isolation.
P10	Lifecycle gates	Entry, exit, owners and conditional decisions.
P11	Supplier obligations	Scope, access, support, changes and findings.
P12	Dependency inventory	SBOM scope, depth, unknowns and effectivity.
P13	Configuration controls	Items, integrity, baselines and change authority.
P14	Development rules	Languages, design rules and exceptions.

ID	Parameter	Required distinction or basis
P15	Build provenance	Inputs, environment, outputs and comparison basis.
P16	Pipeline and signing	Protected gates, secrets and eligible signers.
P17	Tool assurance	Intended use, validation and error detection.
P18	Verification strategy	Methods, representation and acceptance rules.
P19	Coverage and data	Denominators, exclusions and independence.
P20	Timing and resources	Deadlines, budgets, margins and uncertainty.
P21	Identity assurance	Issuance, authentication and revocation.
P22	Privileged access	Scope, duration, review and emergency use.
P23	Cryptographic profile	Algorithms, parameters and protection lifetime.
P24	Key lifecycle	Provisioning, custody, rotation and compromise.
P25	Data handling	Purpose, quality, access and privacy constraints.
P26	Interface semantics	Authority, units, freshness and failure behavior.
P27	Platform trust	Boot, firmware, debug and recovery baseline.
P28	Cloud and service duties	Shared controls, isolation and exit.
P29	Industrial safeguards	Physical effects and product-evidence integrity.
P30	Aviation integration	Flight phases, ground paths and operating limits.
P31	Space and remote operation	Contact, commands, autonomy and restoration.
P32	Model assurance	Domain, data, metrics, safeguards and drift.
P33	AI-assisted work	Permitted use, review and action boundaries.
P34	Deployment profile	Target, hardening, readiness and commissioning.

ID	Parameter	Required distinction or basis
P35	Update and rollback	Activation, interruption, effectivity and recovery.
P36	Monitoring and time	Detection, event schema, capacity and clock quality.
P37	Vulnerability response	Applicability, priority, deadlines and exceptions.
P38	Incident handling	Triggers, authority, evidence and notifications.
P39	Recovery objectives	Time, recoverable state and reconciliation.
P40	Human and remote support	Competence, sessions, workload and handover.
P41	Release and legacy use	Dossier, claims, restrictions and support life.
P42	Retirement and retention	Authority removal, evidence and disposal.
P43	Assurance and publication	Review programme, edition and adoption authority.
P44	Unresolved dependencies	Owner, blocked scope, next action and review.

B.2 Common record payload

Every significant record shall identify a unique ID, object and configuration, purpose, owner, creator, date/time basis, source requirements, evidence, decisions and authentication reference. Attachments shall have stable identities and versions. Superseded evidence, adverse results and changes shall remain traceable.

B.3 Cross-record consistency

Requirements, assets, builds, deployed instances, findings and releases shall agree on identity and state. A migration or restore shall preserve relationships and restrictions. An unresolved discrepancy shall be a controlled gap, not silently normalized to a favorable status.

Annex C - Context, classification and integrated risk dossier

Status: Normative within the proposed AF 9500 requirement set.

C.1 Context model

The dossier shall state intended use, functions, users, modes, mission phases, assets, interfaces and dependencies. It shall identify physical, trust and organizational boundaries and temporary or maintenance paths. Each assumption shall have an owner, basis and invalidation trigger.

C.2 Scenario record

Table C-1. Hazard-threat scenario payload

Element	Required content
Scenario	Fault or threat, access conditions and affected mode.
Mechanism	Vulnerable behavior, propagation and common dependencies.
Consequence	Safety, mission, data and continuity effects with uncertainty.
Controls	Prevention, detection, protective behavior and recovery.
Evidence	Requirement links, representative verification and limitations.
Decision	Residual exposure, eligible authority, restrictions and review.

C.3 Safety-security reconciliation

The assessment shall compare adverse effects of the threat with adverse effects of proposed protective actions. It shall identify the permitted behavior during lost trust or availability and verify transitions. An unresolved conflict shall block the dependent architecture or operation decision.

C.4 Assurance assignment

Classification shall determine evidence depth, independence, representative testing and operational monitoring. The dossier shall explain why the assigned controls are sufficient for each essential scenario and identify unresolved coverage. Numerical ranking shall not replace this argument.

Annex D - Requirements, interfaces and traceability payload

Status: Normative within the proposed AF 9500 requirement set.

D.1 Requirement record

Each requirement shall identify origin, rationale, object, applicable modes, required and prohibited behavior, verification method and acceptance criteria. Derived requirements shall identify system approval. Unresolved ambiguities shall remain visible.

D.2 Trace row

Table D-1. Traceability minimum content

Field	Required content
Requirement	Stable ID, baseline, source and applicability.
Implementation	Design, code, model, data or configured-control reference.
Verification	Method, case, environment, expected and actual evidence.
State	PASS, FAIL, HOLD or approved N/A with rationale.
Review	Eligible reviewer, limitations and remaining actions.
Effectivity	Release and deployed population represented.

D.3 Interface record

The interface record shall include peers, trust, authority, semantics, units, ranges, freshness, timing and adverse-input behavior. Shared assumptions and change notification shall be agreed by both sides.

D.4 Coverage reconciliation

The organization shall account for every applicable essential requirement and explain excluded or deferred items. Bidirectional trace exercises shall demonstrate actual relationships. A percentage shall retain its denominator and shall not conceal a critical gap.

Annex E - Supply, dependency and provenance dossier

Status: Normative within the proposed AF 9500 requirement set.

E.1 Supplier agreement

The agreement shall identify supplied scope, versions, intended use, evidence, support, change notification, vulnerability handling, incident cooperation and exit needs. The receiver shall retain integration and acceptance duties.

E.2 Dependency inventory

The inventory shall bind to the actual artifact and state component identities, relationships, origin, inclusion or runtime status, known gaps and creation method. The organization shall preserve historical inventories for affected-release tracing. Unknown components shall not be omitted from completeness claims.

E.3 Build record

Table E-1. Build and release provenance

Element	Required content
Inputs	Source, dependencies, configuration, models and data identities.
Environment	Tools, versions, options, worker and controlled conditions.
Execution	Authorized trigger, actual actions, logs and deviations.
Outputs	Artifact identities, digests and manifest relationships.
Evidence	Gate results, review, reconstruction and limitations.
Trust	Signing authority, trust policy and compromise dependencies.

E.4 Applicability and affected outputs

A vulnerability or compromise assessment shall connect the finding to actual component, build and deployment states. The record shall distinguish confirmed, excluded and unresolved applicability and identify required containment or communication.

Annex F - Verification, tool and anomaly evidence

Status: Normative within the proposed AF 9500 requirement set.

F.1 Method and tool basis

The dossier shall identify the intended property, method capability, tool baseline, expected results and independent error detection. Models shall retain assumptions, abstractions and implementation relationships. Formal results shall state the exact property and unproven conditions.

F.2 Execution record

Records shall identify target configuration, environment, inputs, authorization, expected and actual outcomes, raw evidence, timing basis and deviations. Security examinations shall retain approved boundaries and stop conditions. Invalid and interrupted runs shall remain in the chronology.

F.3 Anomaly disposition

Anomalies shall retain observation, reproducibility, affected scope, classification, causal evidence, corrective action and regression. The authority shall identify whether a test, tool, requirement or product was defective. A passing rerun shall not erase unresolved earlier behavior.

F.4 Conclusion

The report shall reconcile requirement and structural coverage, test-data validity, findings and residual gaps. Review shall identify what the evidence demonstrates and what remains unknown. The conclusion shall not exceed the tested or analytically justified scope.

Annex G - Identity, cryptography and trust-control records

Status: Normative within the proposed AF 9500 requirement set.

G.1 Identity and privilege record

The record shall identify principal, owner, purpose, credential or identity reference, permitted objects and actions, authentication basis, approval, effective conditions and termination. Reviews shall reconcile actual and approved access. Secrets shall not be included in the record itself.

G.2 Key and trust inventory

Inventory shall identify key or trust-anchor reference, purpose, algorithm/profile, custodian, protected location, permitted operations, cryptoperiod or review basis, backup/recovery and revocation dependencies. Private key material shall remain in approved protected storage.

G.3 Emergency and offline use

Each use shall identify triggering condition, scope, operator, actions, time basis, restrictions and later reconciliation. Cached trust or revocation information shall identify freshness and permitted operation. Emergency arrangements shall have demonstrated limits and termination.

G.4 Compromise and migration

The dossier shall identify affected signatures, artifacts, sessions and assets, assessment uncertainty, containment, replacement and verification. Migration shall preserve compatible boot, update and recovery behavior and necessary historical evidence.

Annex H - Deployment, update and rollback dossier

Status: Normative within the proposed AF 9500 requirement set.

H.1 Deployment baseline

The dossier shall identify artifact, target hardware, firmware, configuration, dependencies, credentials, allowed services, interfaces and monitoring. Prerequisites, operational windows and eligible authorities shall be explicit. Local exceptions shall retain their technical rationale and limits.

H.2 Update transition matrix

Table H-1. Required update transition evidence

Transition	Required evidence
Transfer to staged package	Authentic source, complete bytes and target binding.
Staged to validated	Integrity, signer authority, prerequisites and compatibility.
Validated to installed	Approved mode, protected state and completed installation.
Installed to active	Controlled activation and known behavior on interruption.
Active to confirmed	Actual version, health, restrictions and operational evidence.
Failed to recovered	Trusted compatible recovery and reconciled persistent state.

H.3 Interruption and rollback

Evidence shall cover relevant loss of power, connectivity, storage, credentials and dependent services. Rollback shall address data schema, counters, trust and vulnerabilities. Anti-rollback controls shall not destroy the approved recovery route. Unsupported combinations shall remain blocked.

H.4 Fleet reconciliation

The record shall distinguish not targeted, pending, staged, failed, active, confirmed and unreachable instances. Expansion or stop decisions shall state their evidence and population. Delivery acknowledgment alone shall not close an update.

Annex I - Monitoring, vulnerability and incident records

Status: Normative within the proposed AF 9500 requirement set.

I.1 Monitoring and detection

The plan shall identify conditions, sources, time quality, coverage, capacity, validation and response owners. Blind spots shall have restrictions or alternative arrangements. Detection results shall retain true and false outcomes with defined denominators where performance is claimed.

I.2 Vulnerability assessment

The record shall identify report source, affected component and configuration, exposure, applicability evidence, consequence, uncertainty, treatment, deadline basis and authority. Temporary acceptance shall identify compensating controls, expiry or triggers and verified continuing conditions.

I.3 Incident chronology

Table I-1. Incident and evidence minimum content

Element	Required content
Identity	Incident, assets, configuration, owner and discovery.
Chronology	Observations, actions, time basis and uncertainty.
Scope	Confirmed and potentially affected systems, outputs and users.
Evidence	Origin, integrity, custody, access and preservation limits.
Decisions	Containment, operating restrictions, authority and rationale.
Communication	Recipients, facts, uncertainty, acknowledgment and updates.
Recovery	Trusted-state evidence, residual restrictions and closure.

I.4 Closure and learning

Closure shall reconcile affected populations, remediations, notifications and residual uncertainty. Corrective actions shall address demonstrated causes and verify effectiveness. Restored service or a sent advisory shall not alone establish closure.

Annex J - Recovery, continuity and state reconciliation

Status: Normative within the proposed AF 9500 requirement set.

J.1 Recovery basis

The dossier shall define recovery-time and recovery-point objectives, clock boundaries, minimum service, permitted degradation and consistency requirements. It shall identify all dependencies needed to restore the actual function, including identities, keys, licenses and people.

J.2 Recovery exercise

The exercise shall identify starting condition, selected copies, environment, actions, measured times, restored state, adverse cases and limitations. Evidence shall demonstrate usability and integrity, not only successful copying. The authority shall explain how the exercise represents the intended disaster or compromise scenario.

J.3 Semantic reconciliation

The record shall reconcile commands, transactions, configuration, product results, privileges and externally issued decisions across the interruption. Duplicate execution, stale state and silent data loss shall be checked. Unreconciled items shall retain owners and blocked scope.

J.4 Return to service

Restart shall state exact configuration, verified functions, restrictions, monitoring and eligible approval. Recovery objectives not achieved shall remain findings. The organization shall update capacity, procedures and dependencies and verify corrective action.

Annex K - Machine-learning and AI-assisted-work dossier

Status: Normative within the proposed AF 9500 requirement set.

K.1 Model-use specification

The dossier shall identify intended decisions, domain, consequences, prohibited use, supervision and fallback. It shall bind deployed identity to architecture, weights, preprocessing, thresholds, data and dependencies. External-model evidence gaps shall be explicit.

K.2 Data and evaluation

Records shall retain data origin, rights or restrictions, labeling, splits, transformations and population coverage. Evaluation shall distinguish tuning and independent assessment and disclose leakage risks. Metrics shall identify subpopulations, denominators, uncertainty and consequential failure cases.

K.3 Operational change

Monitoring shall identify drift, out-of-domain conditions, safeguards, owners and response thresholds. Retraining, adaptation and threshold changes shall have bounded authority and reevaluation. Human oversight shall be demonstrated under realistic time and workload conditions.

K.4 Assisted development and agents

The record shall state permitted assistance, exposed data, tool access, generated outputs, review and independent verification. Agentic actions shall have explicit boundaries, approval points and recovery. Untrusted instructions and retrieved material shall not gain authority over controlled requirements or operational permissions.

Annex L - Release, continued use and declaration payload

Status: Normative within the proposed AF 9500 requirement set.

L.1 Assurance dossier

The dossier shall connect claims to exact baselines, requirements, architecture, evidence and residual limitations. It shall reconcile supplier components, anomalies, vulnerabilities, risks, deployment and recovery prerequisites. Contradictions shall be resolved or retained as blocked scope.

L.2 Release statement

Table L-1. Bounded digital release content

Field	Required content
Issuer	Eligible authority, organization and authentication reference.
Object	Artifact, digest/version, platform and configuration.
Scope	Intended use, targets, modes and represented population.
Basis	Requirements, evidence dossier and reviewed findings.
Conditions	Restrictions, dependencies, support and recovery needs.
History	Date basis, predecessor, amendments and withdrawal route.

L.3 Continued-use argument

Legacy or vulnerable configurations shall identify actual exposure, compensating controls, support capability and review triggers. The authority shall state permitted operation and replacement or withdrawal conditions. Past successful use alone shall not establish continuing suitability.

L.4 Claims and withdrawal

Claims shall not imply universal cyber immunity, defect-free software or automatic operating permission. A finding invalidating a claim shall trigger affected-output analysis, controlled amendment and necessary communication while preserving historical evidence.

Annex M - Retirement, data disposition and evidence preservation

Status: Normative within the proposed AF 9500 requirement set.

M.1 Retirement scope

The record shall identify physical and digital assets, dependent services, accounts, trust anchors, contracts, data and records. Remaining duties shall have accountable owners. Transfer and retirement shall have separate authority decisions where their effects differ.

M.2 Termination verification

The organization shall verify removal or revocation of access, identities, connections and unintended control authority. Shared credentials and continuing dependencies shall be assessed. A retired hostname, account or resource shall not remain an uncontrolled takeover path.

M.3 Data and key disposition

Disposition shall identify retained, transferred, sanitized and destroyed populations with approved methods and evidence. Sensitive values shall not be reproduced in ordinary disposal records. Required historical evidence and keys needed for legitimate recovery or interpretation shall be retained under controlled responsibility.

M.4 Closure

Closure shall reconcile inventories, backups, subscriptions, suppliers, custody and user notifications. Exceptions shall identify remaining scope and review conditions. Physical destruction or contract cancellation alone shall not establish complete digital retirement.

Annex N - Assurance, publication and local-adoption dossier

Status: Normative within the proposed AF 9500 requirement set.

N.1 Assurance programme

The programme shall identify representative activities, critical objects, independent reviewers, methods and schedules. It shall include adverse cases, supplier boundaries and prohibited digital transitions. Findings shall connect to actual evidence and affected decisions.

N.2 Finding closure

The record shall retain requirement, observation, consequence, correction, causal action, effectiveness evidence and eligible closure. Administrative completion shall not remove a technical restriction that remains justified.

N.3 Publication control

Publication records shall distinguish preparation, technical review, consultation, comment resolution and eligible approval. Edition, identity and effective conditions shall be controlled. No template shall preassign a publication decision, signature or date.

N.4 Local adoption

Adoption shall identify organizational scope, selected clauses, completed P01-P44 baseline, profiles, methods, records, competence and transition. The adopter shall demonstrate implementation using actual evidence. A master list or purchased document set shall not be represented as verified conformity.

Annex O - Reproducible calculations and decision examples

Status: Informative. All values are synthetic and are not mandatory thresholds, actual product results or evidence of operational approval. The method, assumptions and limitations are part of each example.

O.1 Traceability, disposition and denominator control

A baseline contains 120 requirements: 100 PASS, 8 FAIL, 10 HOLD and 2 justified N/A. All 120 have trace rows. For this example, a verified disposition means a valid PASS or FAIL result; HOLD remains unresolved. Different organizations may define another metric, but shall state its meaning.

Applicable requirements = $120 - 2 = 118$

PASS fraction = $100 / 118 = 84.7458\%$

Valid PASS-or-FAIL dispositions = $108 / 118 = 91.5254\%$

Trace-row presence = $120 / 120 = 100\%$

A complete matrix therefore coexists with eight failures and ten unresolved requirements. None of these percentages permits release where an essential condition remains unresolved. Removing HOLD items from the denominator would produce a misleading success metric unless the changed population and purpose were explicitly justified.

O.2 End-to-end latency budget

A synthetic control path has approved conservative bounds of 8 ms acquisition, 12 ms computation, 4 ms authentication, 9 ms communication and 15 ms actuation. A separate non-overlapping allowance of 5 ms covers relevant jitter and interference. Assume the stages are sequential and these bounds are valid for the same operating conditions.

Total bound = $8 + 12 + 4 + 9 + 15 + 5 = 53$ ms

Margin to a 60 ms deadline = $60 - 53 = 7$ ms

Margin / deadline = $7 / 60 = 11.6667\%$

This is a deterministic budget calculation, not a measured percentile or probability of meeting the deadline. Parallel stages, correlated delays, omitted queues or double-counted allowances require a different model. A mean benchmark cannot replace the stated conservative bounds. Adding a 9 ms security operation would exceed the deadline by 2 ms under these assumptions.

O.3 Serial-service availability

Assume a service requires both application A and identity service B continuously. Their steady-state availabilities are 0.999 and 0.9995, and their availability states are independent. No offline fallback is credited. For this deliberately simplified model:

Series availability = $0.999 \times 0.9995 = 0.9985005$

30-day period = $30 \times 24 \times 60 = 43,200$ minutes

Expected unavailability = $43,200 \times (1 - 0.9985005)$

Expected unavailability = 64.7784 minutes

A 99.95% target would permit 21.6 minutes over this period under the same accounting definition. The modeled series service does not meet that target. Shared outages, nonstationary behavior, planned downtime rules and actual recovery performance can invalidate the simple model. A contractual availability promise is not measured system evidence.

O.4 Detector precision and base-rate effects

A representative evaluation contains 100,000 observation windows, including 1,000 true adverse windows and 99,000 ordinary windows. A detector catches 90% of adverse windows and incorrectly alerts on 1% of ordinary windows. Assume labels are valid and each window uses the same declared rule.

True positives = $1,000 \times 0.90 = 900$

False negatives = $1,000 - 900 = 100$

False positives = $99,000 \times 0.01 = 990$

Precision = $900 / (900 + 990) = 47.6190\%$

Recall = $900 / (900 + 100) = 90.0000\%$

More than half of alerts in this example are false positives despite the 1% false-positive rate. Response staffing and operating effects therefore need explicit evaluation. Results cannot be transferred to another deployment without examining prevalence, workload, labels and distribution. A detector that misses a critical scenario cannot be accepted solely on aggregate precision.

O.5 Recovery time and recoverable state

A service fails at 10:12. Its latest independently verified consistent checkpoint is 10:00 and there is no usable later transaction journal. Restoration takes 80 minutes, functional and security validation takes 25, and state reconciliation takes 20. These activities are sequential. The locally approved objectives are a 120-minute return-to-service interval from failure and no more than 10 minutes of lost committed state.

Actual recovery interval = $80 + 25 + 20 = 125$ minutes

Recoverable-state gap = $10:12 - 10:00 = 12$ minutes

The time objective is exceeded by 5 minutes and the recoverable-state objective by 2 minutes. A report that counts only the 80-minute file restore would misstate the approved objective. If journals exist, their completeness and replay consistency must be demonstrated before crediting a newer recovery point.

O.6 Event ordering with bounded clock uncertainty

Event A is recorded at 100.000 s with an absolute clock-error bound of 0.004 s. Event B is recorded at 100.006 s with a bound of 0.005 s. Assume the bounds cover the relevant capture times and there is no other ordering evidence.

A actual-time interval = [99.996, 100.004] seconds

B actual-time interval = [100.001, 100.011] seconds

B minus A interval = [-0.003, +0.015] seconds

The intervals overlap. B may have occurred up to 3 ms before A or up to 15 ms after it, so their order is not established by these timestamps alone. These are hard bounds, not standard deviations; combining them by root-sum-square would introduce an unsupported statistical interpretation. Sequence or causal evidence may resolve the order separately.

O.7 Zero observed failures and a statistical bound

In 300 independent Bernoulli trials from a fixed representative population, no failures are observed. Assume constant failure probability and a valid detection rule. The exact one-sided 95% upper confidence bound for that trial failure probability is:

Upper bound = $1 - 0.05^{(1 / 300)} = 0.0099361$

The bound is approximately 0.9936%, not zero. It is a frequentist confidence bound for the stated sampling model, not a probability that software is safe or a universal operational failure rate. Correlated tests, systematic defects, incomplete requirements or nonrepresentative inputs invalidate that

interpretation. Additional deterministic and scenario-based assurance remains necessary.

O.8 Exposure accounting without hidden populations

Ten identified assets remain exposed to a particular unresolved condition for 3 days, and another 20 remain exposed for 7 days. Assume all intervals use the same start/stop rule and do not overlap for the same asset. A separate set of 4 assets has unknown state and is not included in the computed total.

Confirmed exposure = $10 \times 3 + 20 \times 7 = 170$ asset-days

The report shall also state four assets with unknown exposure. Unknown is not zero. Asset-days can describe backlog trends but cannot make a short catastrophic exposure equivalent to a long minor one. Criticality, actual reachability, compensating controls and deadline breaches remain separate decision inputs.

O.9 Log-storage capacity

Assume a sustained 500 events per second, an average stored payload of 600 bytes per event, 30 days retention, two full copies and a 25% additional capacity allowance. Decimal GB and TB are used. Compression, indexes, metadata and variation are excluded unless covered by the stated allowance.

Daily payload = $500 \times 600 \times 86,400 = 25.92$ GB

30-day payload = $25.92 \times 30 = 777.6$ GB

Two copies plus allowance = $777.6 \times 2 \times 1.25$

Planned capacity = $1,944$ GB = 1.944 TB

This calculation does not prove adequate peak ingestion, search capacity or retention during an incident. Measurements must establish actual event distributions, indexing costs, redundancy and failure behavior. Losing a collector or exhausting storage requires a defined response rather than a silent gap.

O.10 Contact-window update feasibility

A remote target receives a 120 MiB package over a 2 Mbit/s link with 60% effective payload efficiency. One MiB is 1,048,576 bytes; one Mbit is 1,000,000 bits. Validation, activation and confirmation require 90, 60 and 120 seconds sequentially after transfer. Assume continuous usable contact and no retransmission beyond the efficiency allowance.

Transfer = $120 \times 1,048,576 \times 8 / (2,000,000 \times 0.60)$

Transfer = 838.8608 seconds

Complete sequence = $838.8608 + 90 + 60 + 120$

Complete sequence = $1,108.8608$ seconds = 18.4810 minutes

A 20-minute window leaves 91.1392 seconds. This nominal margin is not an operational approval: link uncertainty, power, interruption recovery, required reserves and permitted mission phase must also be assessed. Download completion alone does not confirm activation.

O.11 Fleet confirmation and trust migration

A trust update targets 8,000 assets. Of these, 7,400 have confirmed the new active baseline, 200 received the package but have not confirmed activation, and 400 have not been contacted. Assume these populations are mutually exclusive and exhaustive.

Package delivery fraction = $7,600 / 8,000 = 95.0\%$

Confirmed active fraction = $7,400 / 8,000 = 92.5\%$

Unconfirmed or unreachable = $600 / 8,000 = 7.5\%$

Revoking the old trust path may strand some of the remaining assets. The authority must assess their actual state, fallback and exposure before transition. The 95% delivery figure shall not be presented as confirmed migration. A dormant or unknown target remains part of the affected population until dispositioned.

O.12 Aggregate model accuracy and a critical subpopulation

A synthetic evaluation contains 9,950 ordinary cases and 50 consequential rare cases. The model classifies 9,900 ordinary cases and 30 rare cases correctly. Assume valid labels and a fixed evaluation rule.

Aggregate accuracy = $(9,900 + 30) / 10,000 = 99.30\%$

Ordinary-case accuracy = $9,900 / 9,950 = 99.4975\%$

Rare-case accuracy = $30 / 50 = 60.00\%$

Twenty of the 50 consequential cases fail. The high aggregate accuracy cannot compensate for that result. Confidence intervals, representativeness, safeguards and scenario-specific criteria are also needed. The example does not assign an acceptable performance threshold for any aerospace function.

Annex P - Integrated application cases

Status: Informative. The cases and identifiers below are synthetic. They illustrate reasoning and record content and do not represent actual product findings, permissions or approvals.

P.1 A signed update reaches the wrong target

Package PKG-A is authentic and has a valid release signature, but the receiving unit uses a different board and data schema from the approved target. The update gate records HOLD for target compatibility. The signature result remains PASS for authenticity under the stated trust policy; it is not changed to FAIL merely because another prerequisite failed. The owner preserves the attempted target identity, prevents activation and obtains a technically supported compatibility decision or the correct package. The case separates authenticated content from permitted installation.

P.2 A protective lockout affects an essential function

An identity service becomes unavailable during a mission phase. A newly proposed security rule would lock all operators out after a short timeout. The safety-security review identifies loss of essential control as an adverse consequence of that rule. The team evaluates bounded offline authority, local protection and post-reconnection reconciliation under the actual threat model. No universal bypass is approved. The record states permitted mode, authorized roles, lifetime basis, monitored conditions and independent evidence. The original unrestricted lockout proposal remains unacceptable for that phase.

P.3 A build cache supplies an unexpected component

The source baseline is correct, but the build uses a cached binary whose origin cannot be reconciled. The pipeline completed successfully and a developer proposes signing the result. The release owner records HOLD for provenance, isolates the uncertain artifact and traces any earlier outputs that used the cache. A clean rebuild uses independently verified inputs and a controlled environment. The team compares outputs, investigates differences and reviews compromised credentials or cache controls. A successful rebuild does not erase the affected-output investigation.

P.4 A scanner reports a vulnerable dependency

A release inventory identifies component C at version 4.2. A report concerns a behavior present in that version. The operator asserts that the vulnerable path is unused. The applicability review examines compiled features, actual configuration, remote and maintenance access and possible privilege changes. Until the exclusion is demonstrated, status remains unresolved. A justified exclusion records its configuration assumptions and change triggers. An exploitable or uncertain deployment receives treatment and restrictions appropriate to actual consequence rather than relying only on a generic severity score.

P.5 A restored test system has lost product relationships

A factory test server is restored and its application starts. However, some result files no longer link to article serial numbers and the approval history is incomplete. Availability is restored, but the product-evidence function is not. The owner records HOLD on affected release decisions, reconciles article, method, configuration and result identities and identifies potentially issued statements. Representative semantic recovery tests are repeated. The return-to-service decision specifies which functions and populations are restored and which remain restricted.

P.6 An AI assistant produces plausible tests

An assistant generates code and a matching test suite. Both assume an incorrect unit conversion, so every generated test passes. Independent review of the authoritative interface requirement exposes the shared error. The team corrects implementation and expected results, checks other outputs from the same assumption and repeats independent requirement-based testing. The record identifies the assistant use and review, while the actual engineering authority retains responsibility. Test quantity and fluent explanations do not establish independent assurance.

P.7 A satellite acknowledges a download

A spacecraft acknowledges receipt of a new package near the end of a contact window. Activation and health confirmation have not occurred. The ground register records STAGED rather than CONFIRMED. Operators preserve the known state and avoid repeating a potentially consequential activation command without the approved sequence and authority. The next contact reconciles package identity, command history and observed state. The case demonstrates why delayed telemetry and lost acknowledgment require explicit uncertainty rather than an assumed successful update.

P.8 A model performs well except in a rare condition

A classifier has high aggregate accuracy, but a critical low-visibility condition is poorly represented and shows consequential failures. The model owner records a domain restriction, examines whether a verified fallback can handle that condition and expands independent evaluation. Synthetic training data may help development but does not automatically establish real-world representativeness. The release argument identifies the actual operating domain and monitors its boundaries. Adding a human reviewer is not sufficient unless the reviewer can recognize the condition and intervene in time.

P.9 A legacy controller cannot accept the current patch

The controller's approved process timing is incompatible with a proposed patch. The owner retains the vulnerability finding and assesses temporary isolation, monitored maintenance access and constrained operating modes. The assessment examines alternate paths and demonstrates the selected controls. A bounded continued-use decision identifies residual exposure, review triggers and a replacement plan. The organization does not report the controller as patched or generally secure. A new threat or failed isolation assumption reopens the decision immediately.

P.10 A retirement leaves a trusted service account

A hosted service is shut down, but its administrative account and signing permission remain active. The retirement review identifies the residual authority and traces shared credentials and dependent systems. The owner revokes or replaces the affected trust, verifies denied access and preserves required historical evidence. Inventory, subscriptions, backups and external integrations are reconciled. The record distinguishes service shutdown from completed secure retirement.

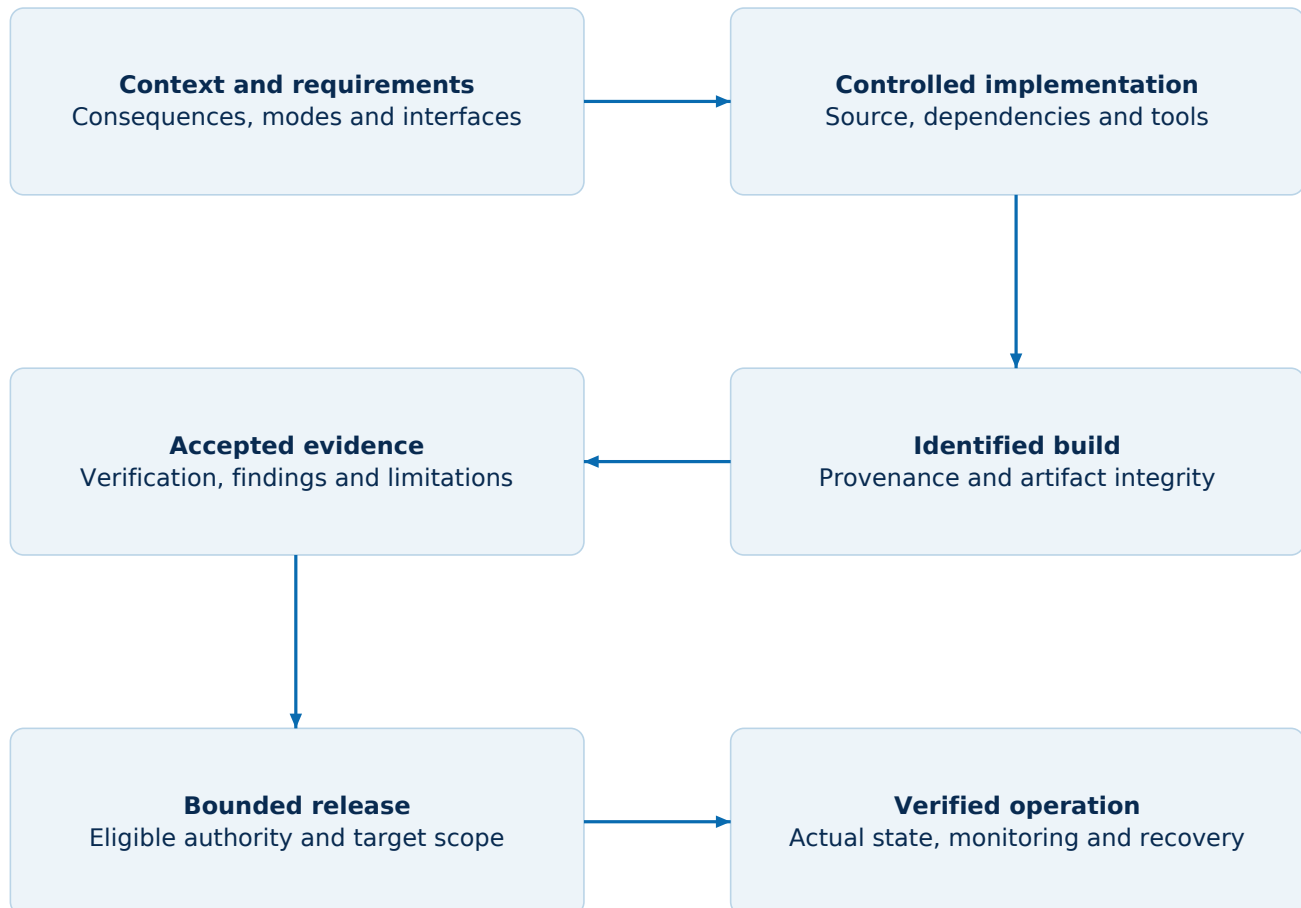
Table P-1. Example populated decision record for Case P.1

Record field	Synthetic entry
Object	PKG-A / target UNIT-17 / board baseline B2.
Required condition	Approved target and schema compatibility before activation.
Observed evidence	Manifest allows B1; UNIT-17 reports B2; no accepted bridge evidence.
Disposition	HOLD on activation; signature verification remains a separate PASS.
Required action	Technical compatibility assessment or correct package; preserve attempt log.
Authority boundary	Eligible deployment authority to review actual evidence; no approval pre-entered.

Annex Q - Digital assurance and decision diagrams

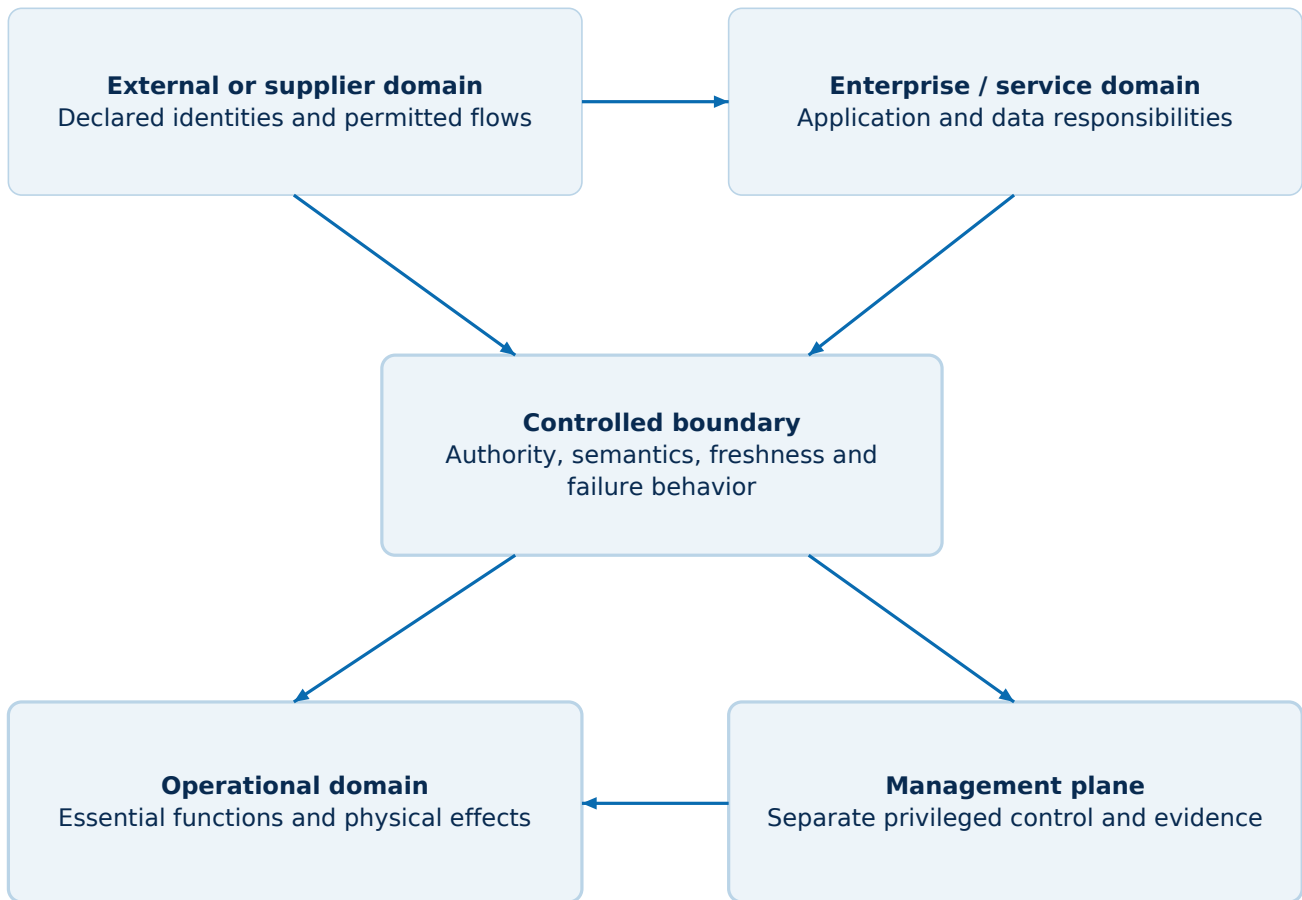
Status: Informative. These diagrams summarize relationships. Applicable requirements and local parameters remain in the main clauses and normative annexes.

Q.1 Requirement-to-operation assurance chain



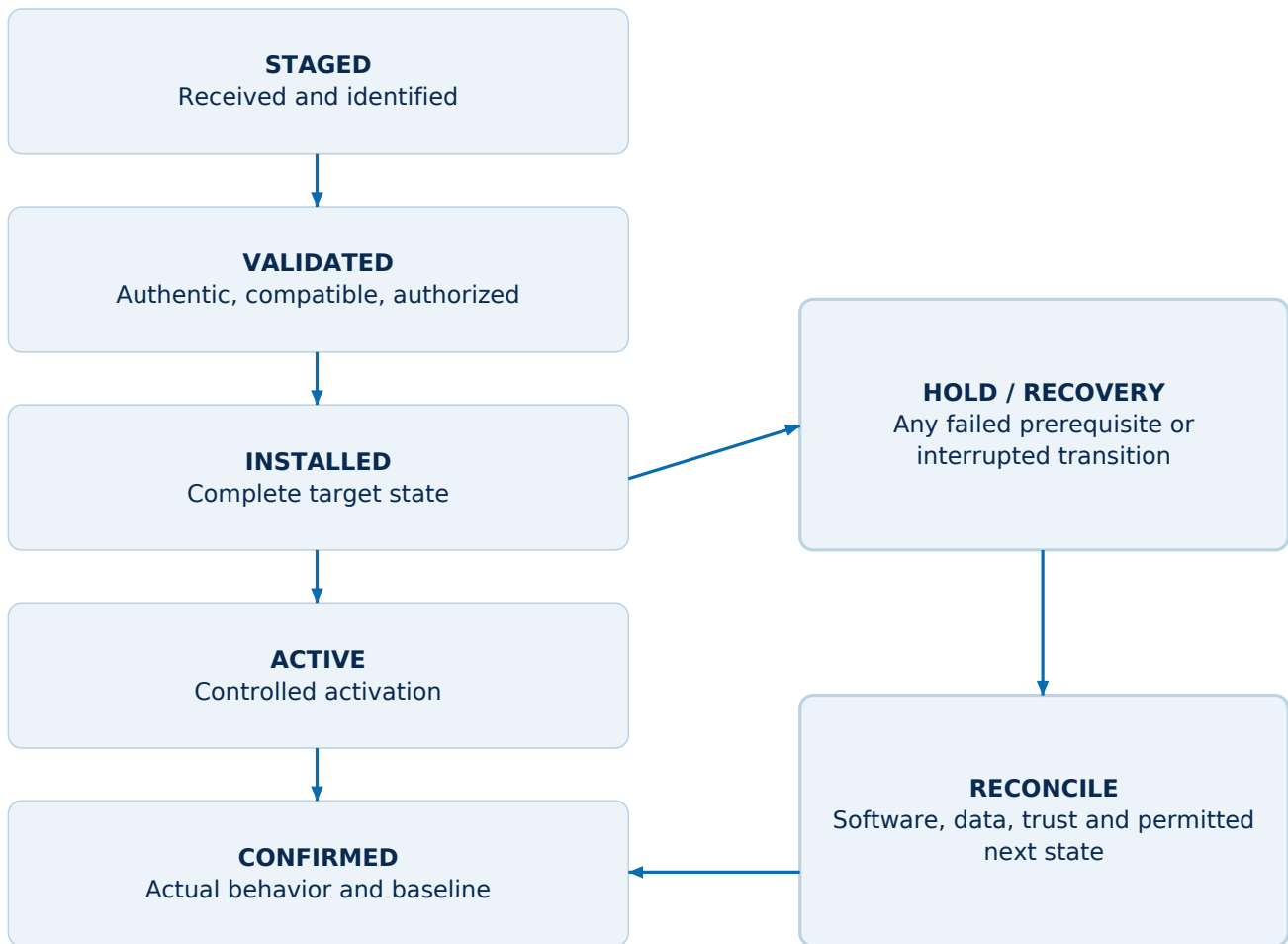
Release binds a defined artifact and configuration to accepted evidence. Operations supply new facts that can invalidate assumptions and reopen the affected claims.

Q.2 Trust boundaries and separate control planes



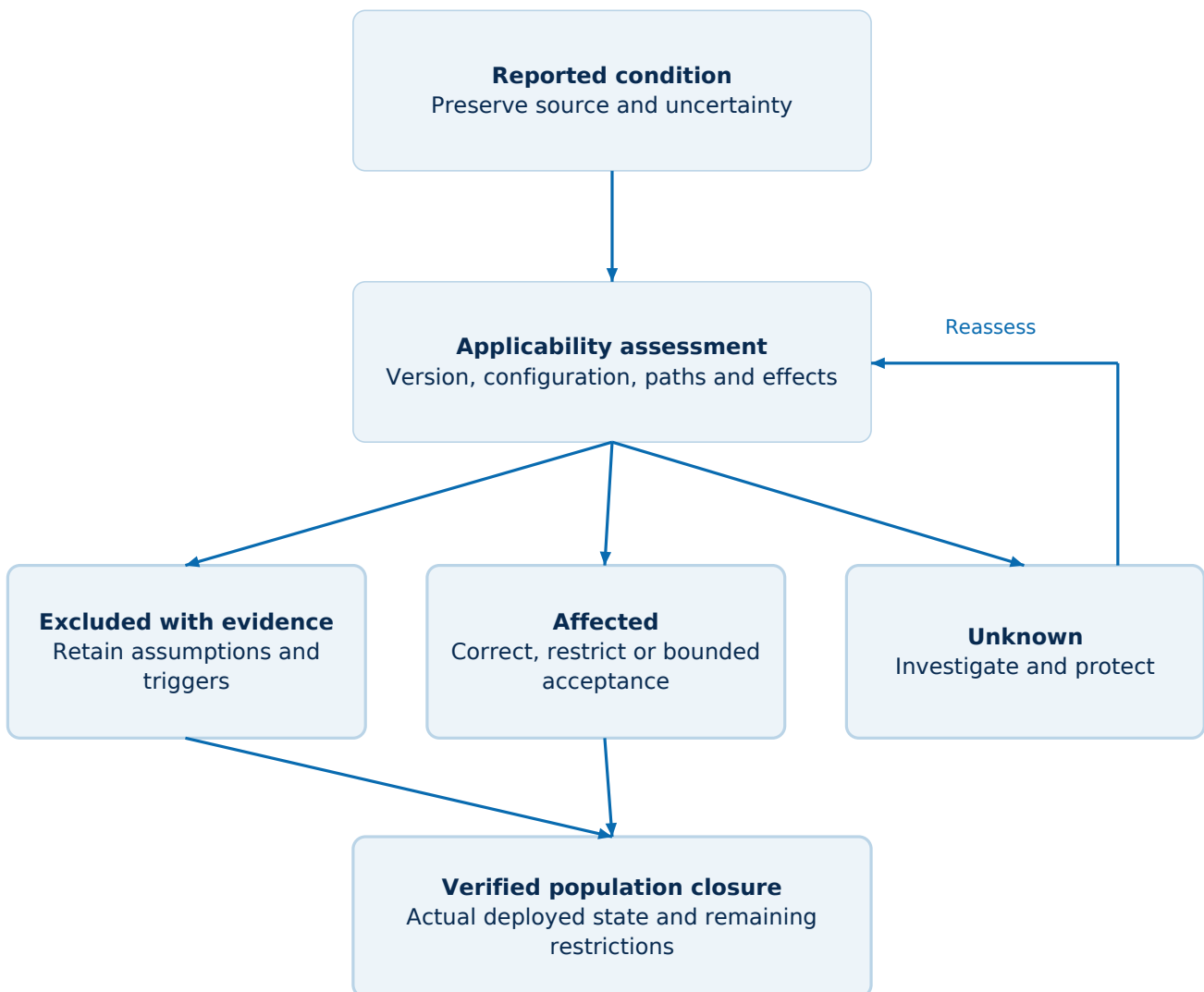
Every crossing requires a justified purpose and control. Separate application networks do not prove isolation if a shared privileged management path can alter both domains.

Q.3 Controlled update and recovery states



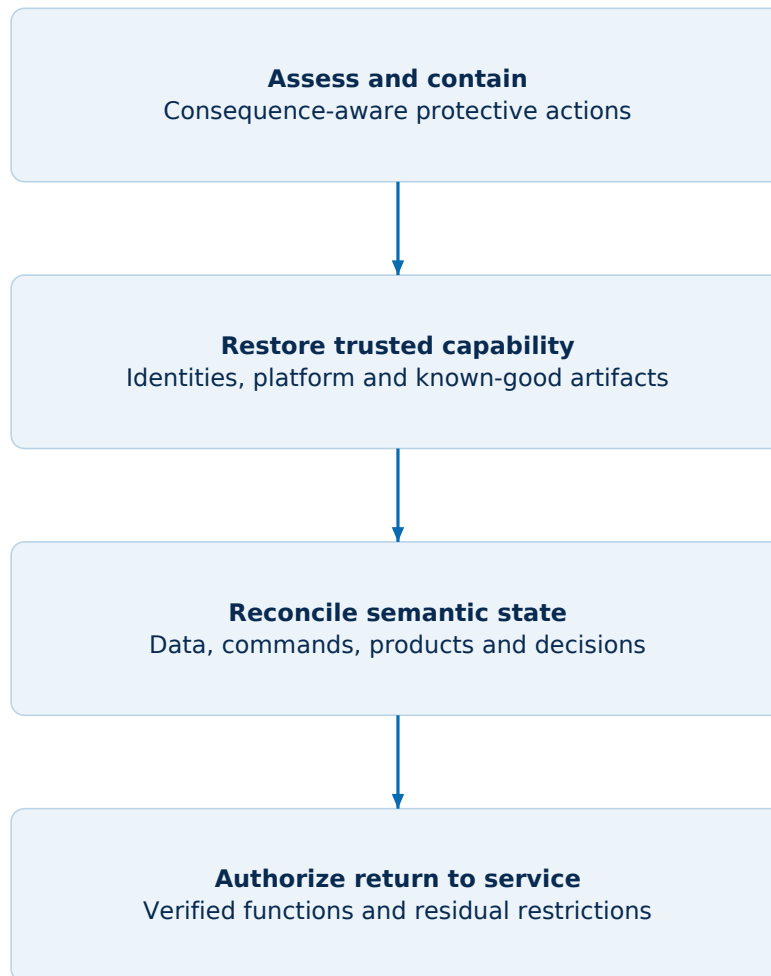
Transfer, validation, installation, activation and confirmation are distinct states. Recovery must preserve compatible software, data and trust, including interruption cases.

Q.4 Vulnerability applicability and bounded treatment



A finding must be connected to actual versions, configuration, paths and consequences. Unknown applicability remains unresolved; publication of a patch does not establish fleet closure.

Q.5 Incident recovery and semantic reconciliation



Return to service requires trusted identities, configuration, data relationships and actual function. File restoration or a running process is only part of that evidence.

Annex R - Activity-based implementation routes

Status: Informative. Select every route whose activities are present. A route is navigation guidance and does not waive shared duties.

R.1 Software producer

Start with Clauses 4-9 for authority, context, requirements and planning. Apply 10-17 to supply, configuration, development, builds, tools and verification. Add 28 for AI-assisted work and 29-40 for deployment, maintenance, release and retirement. Demonstrate a complete source-to-deployment trail and an adverse-change case.

R.2 Component or platform supplier

Define the exact supplied function, target environment, assumptions and evidence limits. Apply 10-17 and 22 as relevant. Provide release-linked dependency and provenance records and support the receiver's integration assessment. Plan vulnerability communication, support continuity and withdrawal without claiming approval of the whole aircraft or mission.

R.3 Airborne and aviation ground integrator

Use 5-8 and 17-22 to establish consequence, boundaries, timing, authority and interfaces. Apply 25 and the actual deployment/update/operational clauses. Demonstrate phase-specific degraded behavior, ground-path controls and a reconciled fleet configuration. Coordinate system safety and operational permissions separately.

R.4 Space or remote mission operator

Apply 5-8, 17-22 and 26 to segment trust, delayed communication, command state and autonomy. Demonstrate update and recovery feasibility for actual contact, power and compute constraints. Retain uncertainty when remote state cannot be confirmed. Include shared ground providers and key lifecycle dependencies.

R.5 Industrial, test and maintenance owner

Apply 24 alongside shared controls. Protect programs, recipes, tools and article-linked results. Assess patching and monitoring for physical effects. Exercise a recovery that reconciles work in progress and issued product records. A restored network shall not be treated as restored product-release evidence.

R.6 Cloud or digital-service operator

Apply 18-23 and 29-39 to responsibility allocation, identities, data, configured isolation, drift, monitoring and recovery. Demonstrate the complete service, including identity and key dependencies. Test an exit or restoration route that preserves independently usable data and authority.

R.7 Model provider or AI-function integrator

Apply 27 with lifecycle, data and verification controls. Establish intended domain, dataset provenance, independent evaluation, safeguards and change boundaries. Examine critical subpopulations and realistic human intervention. Treat model, preprocessing and threshold changes as potentially changed behavior.

R.8 AI-assisted engineering or agent workflow

Apply 28 with tool, access, development and release controls. Define permitted assistance, sensitive-data boundaries and action limits. Preserve generated-output review and independent evidence. Demonstrate that untrusted retrieved instructions cannot grant operational authority or bypass required approvals.

R.9 Assessor, security examiner or assurance owner

Use 4, 9, 14-16 and 39 to define competence, independence, authorized methods and representative evidence. Follow end-to-end and adverse trails. Identify what was demonstrated, what remains uncertain and which decisions are blocked. Do not equate completed templates with effective implementation.

Annex S - Interpretation questions and boundary examples

Status: Informative. Answers explain recurring boundaries and do not supply missing local parameters or waive applicable requirements.

S.1 Does a valid signature make software safe?

No. It supports a defined authenticity claim under the trust policy. Correct behavior, target compatibility, current signer authority and permitted use require separate evidence.

S.2 Does 100% code coverage prove correctness?

No. Executed code may still implement an incorrect requirement or produce a wrong result. Coverage needs valid requirements-based tests, meaningful expected outcomes and review of uncovered or excluded behavior.

S.3 Can an SBOM establish absence of vulnerabilities?

No. It identifies components and relationships within its declared scope. Completeness, vulnerability applicability, configuration and ongoing threat information require separate assessment.

S.4 Can an urgent patch bypass safety checks?

Urgency changes response priority, not the need for eligible authority and a justified technical transition. Interim restrictions and compensating controls may be necessary while a safe update route is established.

S.5 Is fail-closed always the secure answer?

The required protective behavior depends on consequence and operating mode. Blocking access can itself remove an essential control function. The safety-security interaction must be assessed and verified.

S.6 Does restoring a backup close an incident?

No. Trust, persistence, identities, data relationships, pending actions and affected outputs must be assessed. Return to service and incident closure are distinct decisions.

S.7 Can a generic vulnerability score decide aircraft operation?

It is one input. Actual installed state, exposure, functional effects, protective controls, uncertainty and operating authority determine the bounded decision.

S.8 Does a cloud provider's approval cover our application?

No. The configured service and retained user responsibilities require evidence. Application behavior, identity, data, integration and recovery may remain the customer's duties.

S.9 Does a human reviewer make an AI function acceptable?

Only when the reviewer's information, competence, time, workload and ability to intervene are demonstrated for the relevant conditions. Nominal human presence is not an effective safeguard by itself.

S.10 Can old software remain in service without source code?

Only within a justified continued-use argument that addresses evidence limitations, current exposure, support, controls and withdrawal conditions. Previous successful operation alone is insufficient.

S.11 Can an agent approve its own deployment?

Only authority explicitly established in a validated workflow can permit an action, and required independent or human decisions remain mandatory. A generated completion message cannot grant new authority.

S.12 Does this set confer AF recognition or operating permission?

No. Publication, organizational adoption, technical acceptance, recognition and operating permission are separate decisions made by their eligible authorities on the required evidence.

Annex T - Requirement families and implementation crosswalk

Status: Informative. The supporting master list and coverage matrix provide the complete working-document route.

T.1 Requirement families

Table T-1. Core navigation map

Requirement family	Clauses	Main normative annexes
Scope, language and governance	0-4	A-B, N
Context, risk, requirements and architecture	5-8	C-D
Lifecycle, supply and configuration	9-11	D-E
Development, build and tool assurance	12-14	E-F
Verification, coverage and timing	15-17	D, F
Identity, trust, data and interfaces	18-21	D, G
Platforms, cloud and industrial systems	22-24	C, G-H
Aviation and remote space integration	25-26	C-D, H-J
Models and AI-assisted work	27-28	F, K
Deployment and updates	29-30	H
Monitoring, vulnerabilities and incidents	31-33	I
Recovery and human operations	34-35	J
Release, legacy and retirement	36-38	L-M
Assurance, publication and adoption	39-40	N

T.2 Implementation order

Select a representative end-to-end digital function. Establish scope, authority, parameters, assets and consequences. Trace requirements through actual source, build, verification and deployment. Exercise an adverse update, vulnerability, incident and recovery. Expand only when the necessary controls and interfaces for the additional scope are demonstrated.

T.3 Completeness questions

Can the organization identify what was required, what actually executes, which evidence applies and who can decide? Can it identify every affected artifact and deployment when a source, key, component or assumption becomes suspect? Can it recover data meaning, control authority and operational state? Unresolved answers identify assurance gaps even where individual documents appear complete.