



AF 9100:2026

Aerospace Quality Management System

MANUAL

Records, Digital Evidence and Long-Life Continuity Manual

AF-HB-9100-003

FIRST EDITION

30 September 2026 | English master text

Publication identity and application

Control	Publication value
Title	Records, Digital Evidence and Long-Life Continuity Manual
Document code	AF-HB-9100-003
Edition / language	FIRST EDITION / English master text
Companion edition identity	30 September 2026
Controlling source	AF 9100:2026 — FIRST EDITION — 29 September 2026
Responsible owner function	Evidence and records custodian
Primary source anchors	7.8, 7.9, 7.10, 7.11, 7.12, D, O, Y, AJ
Delivery status	Prepared implementation companion. Actual approval, adoption, effectivity and operational decisions are recorded separately.

Use and document-control boundary

This companion implements the supplied AF 9100 requirement basis without changing the original standard. Its process allocation, examples, checklists and record design are authored implementation material. Actual mission or product limits, specialist procedures, permissions and genuine observations must be completed before consequential use. Applicable source minima and independent decision conditions cannot be reduced by this companion.

The printed edition date identifies the companion series; it is not evidence that later preparation, review or operational decisions occurred on that date. New support codes in this set are proposed allocations for controlled registration. Established AF-IG-9100-001, AF-FAQ-9100-001 and AF-TR-9100-001 identities are retained; earlier files, the corporate master list and ASTRA codes are not overwritten.

Equivalent combined or digital records are permitted when all required fields, relationships, authority and history remain intact. A completed PDF field or typed name is not evidence of an authenticated approval. Blank records in this delivery contain no invented applicant, signature, event or result.

Contents and reading route

Publication identity and application	2
Contents and reading route	3
1 Scope, responsibility and source priority	4
2 Operating architecture and controlled outputs	4
3 Required information entities and custody	4
4 Detailed operating modules	4
5 Continuing controls and critical timing	8
6 Independent closure and launch readiness	9
Appendix A — Controlling source and evidence	10
Source tables — complete field and decision payloads	16
Appendix B — Local implementation and release	22
Select actual scope → complete application criteria → use the applicable procedure and technical book → capture authentic evidence → evaluate every applicable condition → obtain the required independent decision. Document availability does not establish implementation or conformity.	

1 Scope, responsibility and source priority

Applies to the responsible function and exact evaluated object selected from the source. Use only the duties triggered by actual activity and retained responsibility.

Boundary	Required implementation decision
Object and route	Identify ORG, PRD, SVC, PRC, PER, SUB or CAB separately. Combined records do not merge outcomes.
Activity	Apply source technical modules by performed or retained responsibility, including relevant outsourced work.
Authority	Technical release, employer task permission, independent attestation and statutory authorization remain distinct.
Source priority	AF 9100:2026 and all compatible binding obligations control. This companion does not import ASTRA programme rules or external normative schemes.

2 Operating architecture and controlled outputs

Layer	Accountable result
Govern and scope	Named responsibility, correct object route, obligations, applicability and available resources.
Engineer and prepare	Approved requirements, qualified methods, competent people and controlled suppliers.
Execute and preserve	Attributable actual output and raw evidence linked to the evaluated configuration.
Review and decide	Independent technical review and all applicable acceptance gates, with precise scope.
Maintain and learn	Source clocks, changes, incidents, corrective effectiveness, true status and accepted record custody.

3 Required information entities and custody

Record class	Minimum links and control
Requirement / configuration	Stable identity, parent, obligation, exact version, methods and evaluated instance.
Person / assignment	Role, observed competence, period, task limits, current case conflict clearance.
Evidence / finding	Original source, conditions, validity, result, requirement, population and preserved adverse history.
Decision / credential / status	Frozen dossier, actual independent authority, exact scope, event chronology and public projection.
Transfer / retirement	Receiving owner, retained meaning, rights, residual obligations and verification of usable access.

4 Detailed operating modules

AF-PR-9100-001 — Document, Record and Publication Control

Owner: Document control manager. Trigger: Creation, issue, correction, translation, migration, withdrawal or loss of an instruction or evidence record.

1. Classify the information. Separate requirements, operating instructions, blank templates, completed records and public extracts. Assign an owner and a unique identifier; record the source edition and the object that may rely on it.

2. Review before release. The technical reviewer checks mandatory verbs, limits, units, references, annex status and change effects. Escalate changes to a rule or acceptance threshold through the technical amendment route; do not describe them as typographical corrections.

3. Approve and distribute. Record actual approval and effective events separately from the printed edition date. Publish a controlled master, identify authorized recipients and verify that the point of performance can retrieve the applicable version.

4. Protect completed evidence. Retain original values, acquisition time, author, configuration and supporting files. A correction adds its reason, actor and approval without overwriting the original observation; prohibit retrospective completion of unobserved work.

5. Preserve and retrieve. Assign retention from the actual obligation, product life and investigation requirements. Exercise retrieval, export and migration of relationships, not merely the opening of files. Suspend disposal while a preservation duty applies.

6. Withdraw and correct. Remove obsolete copies from unintended use, retain their historical decision links and notify recipients of material corrections. Verify cached, translated and remote copies; source availability alone does not establish local implementation.

Completion boundary: A missing applicable instruction, inaccessible essential evidence or unapproved technical amendment prevents dependent use.

Record handover: AF-FR-9100-001, AF-FR-9100-015, AF-FR-9100-032.

AF-PR-9100-010 — Technical Tools, Data Integrity and Evidence Portability

Owner: Information assurance and tool owner. Trigger: A computational tool, data interface or repository is introduced, changed, recovered or retired.

1. Define intended reliance. Identify the decision, consequence, algorithm, data model, units, interfaces, user roles and functions capable of creating or hiding a defect.

2. Control the baseline. Preserve source or equivalent executable definition, dependencies, parameters, access and version. Record the deployed configuration and distinguish test from live records.

3. Test expected behavior. Use independently calculated known answers plus boundary, missing, malformed, wrong-unit and prohibited-state cases. Include attempts to approve with expired authority or open findings.

4. Verify original evidence. Reconcile ingestion to the actual source, object, version and event time. Identify generated, simulated and reconstructed material; a hash proves neither physical truth nor engineering validity.

5. Test meaningful recovery. Restore identities, configuration links, decisions and events after the recovery point. Reconcile contents and relationships as well as totals. A running application with broken evidence links remains held.

6. Release and preserve. Record actual local acceptance, remaining restrictions, trained users and revalidation triggers. Transfer usable records and accepted custody before cutover; PDFs are record artifacts, not a deployed database.

Completion boundary: Failure of an essential known-answer, authority or relationship check blocks consequential use of the affected tool.

Record handover: AF-FR-9100-019, AF-FR-9100-029, AF-FR-9100-032.

AF-PR-9100-025 — Knowledge Preservation and Lifecycle Learning

Owner: Knowledge and improvement owner. Trigger: New lesson, recurring event, departure of a specialist, source exit or long-life support change.

1. Identify critical knowledge. Map design rationale, process experience, failure mechanisms, source/build environments, support data and tacit skills to actual continuing obligations.

2. Capture usable evidence. Record the original problem, configuration, conditions, analysis, counter-evidence, action and observed result. Separate a lesson's applicability from a general slogan.

3. Review transfer and access. Assign custodians, lawful rights, readable formats, technical dictionaries and replacement expertise. Test whether receiving users can interpret the evidence without the original author.

4. Apply lessons at decisions. Check relevant learning at programme start, design review, purchasing, process change and support planning. Record why a prior solution applies or does not apply to the new context.

5. Verify improvement. Compare actual outcomes against the baseline and adverse effects after controlled implementation. Retain failures and avoid attributing improvement to an action when the measurement basis changed.

6. Monitor continuity and recurrence. Exercise retrieval of current and legacy evidence, track repeated mechanisms and update succession, obsolescence and source-exit arrangements.

Completion boundary: Loss of essential support knowledge or source access holds the claim that depends on it until a valid alternative exists.

Record handover: AF-FR-9100-031, AF-FR-9100-028, AF-FR-9100-032.

AF-PR-9100-026 — Continuity, Emergency Interfaces and Assured Recovery

Owner: Continuity owner and technical return authority. Trigger: Loss of critical staff, supplier, utility, site, data service or protective support.

1. Identify dependencies and failure scenarios. Record critical functions, maximum tolerable interruptions under the real profile, recovery objectives, alternate sources and common failures.

2. Demonstrate contingency resources. Verify available people, authority, equipment, communications, compatible configurations and actual receiving arrangements. An agreement alone does not prove a backup can perform.

3. Plan safe exercises. Define protected test environment, expected outcomes, stop controls and evidence. Include supplier loss and compromise of technical records, not only discussion of an ideal scenario.

4. Contain and preserve during disruption. Record real event chronology, affected configurations and outputs, original evidence and required notices. Keep protective operations distinct from investigation and public status administration.

5. Restore and reconcile. Verify both availability and integrity, including events after the recovery point, life and configuration records, open holds and local readiness. Confirm alternative delivery retains qualified capability.

6. Authorize return and learn. The technical authority approves bounded return only after required checks. Independently update any scheme status, assess prior outputs, repeat failures and verify improvements.

Completion boundary: Availability restored without required integrity or protective evidence does not authorize assured use.

Record handover: AF-FR-9100-029, AF-FR-9100-017, AF-FR-9100-006, AF-FR-9100-008.

AF-PR-9100-027 — Software, AI, Models and Trusted Updates

Owner: Digital technical and security authorities. Trigger: Digital development, model-based acceptance, deployment, update, drift or end of support.

1. Define reliance and authority. Identify requirements, criticality, architecture, domain, users, permitted and prohibited actions, interfaces and recovery. Assess whether the proposed tool is necessary and sufficiently verifiable.

2. Control source and data. Preserve source, logic, build definitions, toolchain, dependency inventory and loaded configuration. For AI preserve dataset rights, labeling, partitions, weights and preprocessing without evaluation leakage.

3. Verify the actual target and domain. Use traced tests, boundary and failure conditions, resource and timing cases, meaningful coverage and independent validation data. A high aggregate score does not close a failed essential scenario.

4. Check defensive integrity. Assess trust, privileges, vulnerabilities, OT compatibility and safety-security conflicts. Intrusive tests require written safe authorization; signatures alone do not establish technical suitability.

5. Release and update predictably. Approve the exact artifact, target, installation, compatibility, interruption response and rollback limits. Verify the deployed state and protect against inappropriate reintroduction of a known unacceptable defect.

6. Monitor, constrain and preserve. Define drift, changed exposure, unavailable inputs and response authority. Reassess adaptation outside the approved envelope; preserve source/build access, records and support beyond supplier or platform exit.

Completion boundary: Unknown target configuration, invalid evaluation or failed essential protection blocks consequential deployment.

Record handover: AF-FR-9100-019, AF-FR-9100-029, AF-FR-9100-005, AF-FR-9100-007.

AF-PR-9100-035 — Surveillance, Renewal, Status, Transfer and Closure

Owner: Scheme continuing-assurance owner. Trigger: Approaching due date, material change, adverse evidence, missed requirement, transfer or operator exit.

1. Establish the real time baseline. Record decision, issue, expiry, completed surveillance and profile-specific conditions separately. Use actual time zone, calendar rules and the shortest interval for inseparable mixed criticality.

2. Plan current technical coverage. Use 12-month C0/C1 or six-month C2/C3 surveillance with actual route-appropriate evidence. Apply ORG resource/site floors separately and PER practical/current-competence conditions where relevant.

3. Act on adverse and overdue conditions. Protect critical concerns immediately, apply the 24-hour critical notices/status controls and verify major/minor closure within source clocks. Booking or payment is not completed surveillance.

4. Control suspension and restoration. State scope, prohibited use, actions and the 90-day final resolution limit. Restore only on evidence, restrict independently unaffected scope or withdraw; preserve original expiry unless full renewal occurs.

5. Complete renewal truthfully. Evaluate current performance, changes, complaints, competence and all in-scope findings before actual renewal. A decision after expiry retains a gap; do not backdate a certificate.

6. Transfer duties and preserve closure. The receiving operator reviews authenticity, scope, history, findings, competence and needed new evaluation. Accept custody of usable records, outstanding remedies and status duties; file transfer does not transfer authority.

Completion boundary: Missed required surveillance or unsupported continuing conformity triggers the applicable affected status action.

Record handover: AF-FR-9100-008, AF-FR-9100-006, AF-FR-9100-009, AF-FR-9100-010, AF-FR-9100-032.

5 Continuing controls and critical timing

Control	Trigger / maximum interval	Evidence and consequence
Ongoing attestation	Independent decision / maximum 24 months	Separate evaluated instance from ongoing validity; a shorter profile or permission can control. AG.1.
C0/C1 surveillance	Decision or last completed surveillance / 12 months	Actual completed route-appropriate work, not booking. AG.2.
C2/C3 surveillance	Decision or last completed surveillance / 6 months	Shortest applicable interval for inseparable mixed scopes. AG.2.
Internal audit programme	Applicable programme / no more than 12 months	C2/C3 critical-control implementation additionally examined within six months. 9.3(d).
Complete management review	Previous full review / no more than 12 months	Serious concerns escalated immediately; focused reviews when warranted. 9.4(c).
Corrective-action plan	Original finding notification / 30 calendar days	Immediate containment remains separate. AG.4.
Major / minor closure	Original finding notification / 60 / 90 calendar days	Verified effectiveness; no reset by reissuing a report or changing owner. AG.4.
Critical holder notice	Awareness / within 24 hours	Earlier binding obligations remain; immediate protective action. AG.4.
Critical operator status action	Substantiated critical concern / within 24 hours	Suspend affected scope or impose a justified effective restriction. AG.4.
Public status update	Status decision / within 2 calendar days	Urgent holder notice is not deferred until registry processing. AG.5.
Suspension resolution	Suspension decision / maximum 90 calendar days	Restore on evidence, restrict independently unaffected scope or withdraw; no administrative restart. AG.5.
Evaluation report	Evaluation close / within 14 calendar days	Record necessary exceptional delay; original finding clocks remain unchanged. AC.7.
Complaint/appeal acknowledgement	Receipt / within 5 calendar days	Urgent safety/integrity triage is immediate. AI.2.
Ordinary appeal submission	Decision notice / normally within 30 calendar days	Reasoned good-cause late admission remains possible. AI.3.
Ordinary determination	Receipt / normally within 60 calendar days	Necessary extension has reasons and progress at least every 30 days. AI.5.
Assessment/decision retention	Last relevant decision / at least 7 years	Longer applicable obligation, life or preservation hold prevails; lawful personal-data handling remains separate. AG.7.
Publication suitability review	Issue / previous review / at least every 3 years	Earlier review after material evidence or inconsistency. Y.6.
Substantive technical amendment	Public consultation / at least 60 calendar days	Actual comments, dispositions, technical checks, adoption and effectivity. Y.3.

These intervals originate in the supplied AF 9100 provisions; application remains route-, role- and event-specific. They are not instructions to delay an earlier protective or binding duty.

6 Independent closure and launch readiness

Review question	Evidence to retain
Authority and responsibility	Actual legal operator, owner, competent technical authority, independent reviewer and permitted result class are recorded.
Scope and criteria	Object, configuration, site, period, trigger, every technical value or observable attribute, units and prospective approval are complete.
Evidence and methods	Original accessible evidence, representative observations, valid methods, uncertainty, adverse cases and limitations support the intended conclusion.
People and independence	Competence is current for each task; genuine conflicts, relevant prior work and needed separation have been checked.
Records and tools	Field meanings, unique IDs, original history, access, retention, recovery and actual deployed workflows have passed local validation.
Decision and public use	All relevant blockers are resolved; required independent decision and written permissions precede the exact public claim.
Continuity and handover	Receiving custody, unresolved duties, corrections and historical decisions survive transfer, retirement or provider closure.

Appendix A — Controlling source and evidence

Source: AF 9100:2026, Aerospace Quality Management System, FIRST EDITION, 29 September 2026; supplied 131-page PDF. Source page references below locate the original publication. These excerpts are read with the complete applicable standard; local implementation sequences do not replace it.

7.8 Organizational knowledge and technical continuity

SOURCE p. 19 | Normative when applicable

7.8(a) The organization shall identify knowledge necessary for current and future obligations, including tacit process knowledge, field experience, design rationale and failure mechanisms. It shall preserve critical knowledge when personnel retire, suppliers exit or technology changes.

7.8(b) Lessons learned shall be indexed so that relevant programs can retrieve and evaluate them. Reuse of a lesson or legacy design shall include an applicability check; similarities in name or appearance shall not establish equivalence of mission, materials or environment.

Required evidence: Knowledge map; succession and transfer records; lessons database; reuse applicability reviews.

7.9 Communication and controlled information exchange

SOURCE p. 19 | Normative when applicable

7.9(a) The organization shall define what information is communicated, by whom, to whom, when and through which controlled channels. Urgent information affecting released products shall have an escalation path and acknowledgement mechanism. Supplier and customer changes shall reach the functions that use the affected data.

7.9(b) Sensitive, proprietary, personal or controlled technical information shall be shared only through authorized arrangements. Meeting attendance or federation membership shall not itself grant access. Communication restrictions shall be reconciled with required hazard and conformity reporting through an approved process.

Required evidence: Communication matrix; notification and acknowledgement logs; approved information-sharing arrangements.

7.10 Document creation, approval and distribution

SOURCE p. 19 | Normative when applicable

7.10(a) Documented information shall have a unique identity, title, revision, owner, approval status and effective date as appropriate. Review shall verify technical accuracy, clarity, consistency and suitability before issue. Instructions shall distinguish mandatory steps, hold points, permitted alternatives and acceptance criteria.

7.10(b) Current information shall be available at the point of use. Obsolete versions shall be removed from unintended use or clearly restricted for historical purposes. Personal copies, local spreadsheets and cached digital files shall be controlled when they influence conformity decisions.

Required evidence: Document master list; approval workflow; distribution controls; point-of-use verification.

7.11 Record integrity, retention and long-life readability

SOURCE p. 19 | Normative when applicable

7.11(a) Records shall preserve the identity of the subject, performer, reviewer and applicable configuration, together with time, results, units and disposition. Changes to recorded evidence shall retain the original value, reason, author and approval where relevant. Electronic signatures and acceptance media shall be individual, protected and revocable.

7.11(b) Retention periods shall consider law, contract, product life, latent defects, liability, material traceability and long- duration missions. No universal short retention period is prescribed. Digital preservation shall address format obsolescence, cryptographic validity, migration verification, backup, recovery and readable access after supplier or platform failure.

7.11(c) The organization shall test retrieval of selected legacy and current records, including restoration from backup. Destruction shall be authorized, recorded and suspended when subject to a relevant investigation, claim or preservation obligation.

Required evidence: Retention schedule; signature controls; audit trails; migration and restore tests; authorized disposal records.

7.12 Technical software, spreadsheets and decision tools

SOURCE p. 19 | Normative when applicable

7.12(a) Software, scripts, spreadsheets and computational tools that influence design, inspection, acceptance or assurance decisions shall be identified and controlled. Validation shall be proportionate to the consequence of an undetected error and shall include known-answer tests, boundary conditions, unit consistency and independent review where required.

7.12(b) Inputs, algorithms, dependencies, versions and output interpretation shall be documented. Formula cells and approved parameters shall be protected where appropriate. An AI-generated calculation or report shall undergo competent review; fluent language or successful execution shall not constitute verification of technical correctness.

Required evidence: Tool inventory; validation plan and known-answer tests; version records; review and revalidation triggers.

D.1 Requirement-record integrity

SOURCE p. 55 | Normative when applicable

D.1(a) Every controlled product or service requirement shall have an identifier, statement, source, owner, revision, rationale, applicability, verification method and acceptance criteria. Derived and safety-related requirements shall include their parent link and approving authority.

D.1(b) The organization shall maintain traceability through allocation, implementation, verification, anomaly resolution and release. Traceability completeness shall be evaluated for meaning and validity, not only the presence of hyperlinks. Broken or circular links shall be investigated.

D.2 Identifiers, versioning and time

SOURCE p. 55 | Normative when applicable

D.2(a) Identifiers shall remain unique within the defined repository and resolvable after migration. Revision and status shall be distinct; an approved obsolete version shall not appear current. Time records shall identify the relevant time basis and sequence sufficient to reconstruct events.

D.2(b) Units, coordinate systems, reference frames and data encodings shall be explicit where misinterpretation could affect conformity. Imported supplier data shall be checked for mapping errors, truncated precision and semantic differences. Automated exchange shall retain validation results.

D.3 Evidence provenance and tamper indication

SOURCE p. 55 | Normative when applicable

D.3(a) An evidence record shall identify the source system or person, acquisition method, processing, transformations and approvals. Cryptographic hashes or signatures may support integrity but shall not be treated as proof that the original observation was correct.

D.3(b) Corrections shall preserve the prior evidence and explain why it changed. Access and modification logs shall be protected in accordance with consequence and obligations. Migration shall verify relationships as well as files; a readable PDF without its underlying configuration links may be insufficient. The filled chain demonstrates structure only. It deliberately does not supply a universal stopping-time value, load or speed; those values require a valid system-specific safety basis.

O.1 Security evidence baseline

SOURCE p. 77 | Normative when applicable

O.1(a) The organization shall maintain the records in Table O-1 for the relevant scope. Evidence shall be versioned and linked to the product, service or infrastructure configuration. Confidential security information shall have controlled access without losing authorized auditability.

O.1(b) The security review shall identify unresolved dependencies and limitations. A security certification or penetration-test report for a different scope shall not establish assurance of the actual deployed system.

O.2 Update release checklist

SOURCE p. 77 | Normative when applicable

O.2(a) Before update deployment, the organization shall verify the approved build, target compatibility, cryptographic origin/integrity, regression evidence, hazard/security impact and required authorization. The

deployment plan shall include interrupted installation and loss-of-power scenarios where relevant.

O.2(b) After installation, the actual version, configuration and protective functions shall be verified. Failed or partial deployment shall remain visible in fleet or asset status. Rollback shall be evaluated for compatibility and vulnerability consequences rather than assumed always safe.

O.3 Incident-to-product linkage

SOURCE p. 77 | Normative when applicable

O.3(a) When an incident could affect engineering data, process programs, test records or released products, the organization shall assess the affected technical population. Cyber response and product-quality response shall share a controlled evidence trail.

O.3(b) Return to operation shall require both operational restoration and justified integrity. The authority making that decision shall understand remaining uncertainty. Unverified records shall not be silently reclassified as authentic because the server has been restored.

O.4 Filled illustrative recovery evaluation

SOURCE p. 77 | Definition, explanation or informative example; no new universal limit

O.4(a) Example recovery objectives are RTO=4 hours and RPO=1 hour for a technical-record service. An exercise restores service in 3.2 hours from a backup 45 minutes old. These two objectives are met in the example, but one configuration-link integrity check fails.

O.4(b) The exercise outcome is therefore “service restored; assured use held pending integrity correction”. Passing time objectives does not establish trustworthy evidence. The record retains the failed check, affected records, corrective action and successful repeat verification.

Y.1 Publication identity and controlled edition

SOURCE p. 99 | Normative when applicable

Y.1(a) The publication identifier shall be AF 9100:2026 and the edition label First Edition. The publication date is 29 September 2026. The publisher designation shall be Aerospace Federation. The full identifier shall be used in conformity statements so that the AF publication cannot be confused with an unrelated document.

Y.1(b) AF is an AF publication-series designation. It shall not be interpreted as adoption by a regional standards system or a claim of regulatory endorsement. Any separate recognition arrangement shall identify its actual parties, scope, date and conditions without altering the meaning of this publication.

Y.1(c) Controlled distribution shall preserve the approved text, tables, equations, figures, annex status and edition metadata. Uncontrolled extracts shall be identified as extracts and shall not be presented as the complete requirement set.

Required evidence: Publication master; edition metadata; controlled copies; accurate extracts and recognition statements.

Y.2 Interpretation requests and technical resolution

SOURCE p. 99 | Normative when applicable

Y.2(a) A request for interpretation shall identify the exact provision, application context, ambiguity, conflicting readings, proposed consequence and relevant evidence. AF shall assign competent reviewers and check conflicts before issuing a controlled response.

Y.2(b) An interpretation may explain an existing requirement but shall not silently create a new obligation, relax a minimum or validate previously missing technical evidence. A material requirement change shall use the amendment process. Where a safe interpretation cannot be established, the affected dependent decision shall remain held or bounded by a lawful technical restriction.

Y.2(c) Issued interpretations shall have unique identifiers, dates, applicable clauses, rationale and approval records. Parties using the standard shall assess their effect on current profiles, procedures and claims and preserve the resulting decisions.

Required evidence: Interpretation request; technical review; controlled response; implementation-impact record.

Y.3 Corrections and amendments

SOURCE p. 99 | Normative when applicable

Y.3(a) An editorial correction shall identify its exact location and show that it does not change technical intent. Changes to requirements, decision rules, thresholds, scope, validity or essential competence shall be treated as technical amendments, not hidden editorial corrections.

Y.3(b) A technical amendment shall include a change rationale, affected clauses and annexes, cross-clause consistency review, relevant technical and mathematical checks, implementation impact and defined effectivity. Substantive changes shall undergo at least 60 calendar days of public comment before final adoption. Comments and dissent shall receive recorded dispositions.

Y.3(c) Urgent safety information may communicate a protective concern and necessary interim measures, but shall be identified separately and shall not silently rewrite this edition. The subsequent amendment shall follow the controlled technical process.

Required evidence: Correction/amendment record; technical and consistency reviews; comment log and dispositions; actual adoption and effectivity.

Y.4 Numbering, translations and technical fidelity

SOURCE p. 99 | Normative when applicable

Y.4(a) AF shall maintain unique clause, table, figure, equation and form identifiers. Renumbering shall preserve a traceable correspondence and shall not invalidate historical evidence references. Cross-references shall resolve to actual provisions and shall identify whether the cited content is normative or informative.

Y.4(b) An authorized translation shall preserve technical meaning, normative verbs, mathematical notation, units, definitions and decision logic. Ambiguities shall be escalated rather than resolved through unrecorded local interpretation. The English text is the reference edition for this publication; any authorized translation shall state its relationship and issue identity.

Y.4(c) Reformatted accessible copies may be issued where the complete content and relationships are preserved. Layout changes shall not alter tables, mathematical signs, figure labels or the association between a requirement and its exceptions.

Required evidence: Numbering and correspondence register; translation review; technical layout verification; controlled accessible copies.

Y.5 Rights, marks and honest publication claims

SOURCE p. 99 | Normative when applicable

Y.5(a) Rights and permissions for reproduction, licensed use and AF marks shall be administered by the responsible rights holder through explicit terms. A copy of the standard shall not itself confer authority to certify, accredit, represent AF or use its marks.

Y.5(b) Publication status shall be distinguished from independent technical validation, regulatory approval and recognition by another party. Claims about completed evaluation or recognition shall require actual supporting records. Adoption of the document by an organization shall not be described as adoption by the whole sector.

Y.5(c) The publisher and scheme operators shall correct misleading publication or recognition statements when identified and shall preserve the record of the correction. No external endorsement shall be inferred from the similarity of a publication number, a technical term or the use of familiar assurance methods.

Required evidence: Actual permissions; mark controls; evidenced recognition claims; corrected misleading statements.

Y.6 Periodic review and maintenance record

SOURCE p. 100 | Normative when applicable

Y.6(a) AF shall review the continued suitability of the edition at least every three years and sooner where significant safety evidence, technology, feedback or implementation inconsistency warrants. A review shall consider technical coverage, decision consistency, proportionality and effectiveness of the scheme.

Y.6(b) The maintenance record shall distinguish proposals, approved changes, editorial corrections, interpretations and superseded content. A future proposal does not modify the current edition before its actual approved effectivity. Holders shall retain the basis used for each historical decision.

Required evidence: Review program; technical feedback; controlled maintenance log; actual effective versions.

AJ.1 Form control and common data fields

SOURCE p. 128 | Normative when applicable

AJ.1(a) Each operational record shall have a unique ID, form type and revision, object or applicant identity, applicable scope and profile, creation and decision dates as relevant, authors, reviewers, approvers, status, evidence references, access class and retention basis. Corrections shall preserve the previous record and the reason for change.

AJ.1(b) An electronic signature shall identify the responsible individual and the approved action. Shared credentials shall not mask accountability. A form's completion status shall not itself establish technical conformity. Required relationships shall remain resolvable after document export or database migration.

Required evidence: Controlled form register; attributable approvals; version and status history; accessible evidence relationships.

AJ.2 Requirement and evidence-status dictionary

SOURCE p. 129 | Normative when applicable

AJ.2(a) Evidence status shall distinguish planned, collected, technically reviewed, accepted for the stated purpose, rejected, superseded and unavailable. "Accepted evidence" means adequate for the identified decision use, not unconditional truth or indefinite validity. A planned test shall not appear as completed evidence.

AJ.2(b) Requirement status shall distinguish conforming, nonconforming, not applicable with approved rationale and not yet demonstrated. An indeterminate measurement shall remain not demonstrated for acceptance until valid disposition; it shall not be silently converted into "not applicable". The status record shall identify the person and basis of change.

Required evidence: Controlled status dictionary; evidence-purpose linkage; approved applicability; attributable state changes.

AJ.3 Completed illustrative profile record

SOURCE p. 129 | Definition, explanation or informative example; no new universal limit

AJ.3(a) The example below concerns a fictional ground-support dimensional inspection service. Its numerical limits demonstrate record structure; they are not prescribed design criteria. The actual technical owner must establish the real application profile before use.

AJ.4 Completed illustrative assessment and decision record

SOURCE p. 129 | Definition, explanation or informative example; no new universal limit

AJ.4(a) This example combines F04–F08 fields to show a traceable decision. The object is an ongoing ORG scope; it is not the same conformity object as the SVC example above. Shared identifiers identify related business activity without merging conclusions.

AJ.5 Completed illustrative personnel and supplier records

SOURCE p. 130 | Definition, explanation or informative example; no new universal limit

AJ.5(a) The examples retain the distinction between demonstrated competence, employer task permission and supplier work approval. They deliberately contain no real personal data, signature or purported live certificate number.

AJ.6 Cross-clause consistency and interpretation controls

SOURCE p. 130 | Normative when applicable

AJ.6(a) The organization and scheme operator shall check that profiles, contracts, internal procedures, calculations, electronic states and public statements agree with the controlling clauses in Table AJ-6. A locally invented workflow shall not change a requirement simply because it is convenient to automate.

AJ.6(b) Detected contradictions shall be recorded with affected objects and versions, evaluated for technical and status impact, and corrected through authorized change. Where a safe resolution is not yet available, dependent acceptance or attestation shall be held. Historical records shall remain truthful.

Required evidence: Consistency review; identified conflicts; impact assessment; approved corrections; preserved historical decisions.

AJ.7 Digital implementation and record export

SOURCE p. 131 | Normative when applicable

AJ.7(a) A digital workflow shall implement required state transitions, approvals and access controls and shall be tested against permitted and prohibited cases. Tests shall include open critical findings, expired competence, unavailable evidence, mismatched configurations, suspended status and an attempted unauthorized approval.

AJ.7(b) An export shall preserve readable decisions, identities, configurations, requirements, actual results and relationships to supporting evidence. A summary PDF without the necessary source evidence shall not be described as a complete transferable dossier. Migration and restoration shall verify records and relationships, not merely file counts.

Required evidence: Workflow validation; prohibited-case tests; attributable approvals; complete exports; relationship and recovery verification.

Source tables — complete field and decision payloads

Table D-1 — Required lifecycle data entities

Source p. 55 | Required structure when applicable

Entity	Minimum fields	Required relationships
Requirement	ID; revision; statement; source; rationale; criticality; owner; acceptance criterion; status.	Parent need; allocated item/function; verification case; applicable obligation.
Configuration item	ID; type; revision; physical/software identity; owner; baseline; approved use.	Requirements; BOM; interfaces; change history; as-built or deployed instances.
Material or component lot	Source; manufacturer; lot/batch; quantity; condition; certificate; received date.	Incoming verification; process route; consumed serials; split/merge history.
Verification case	ID; method; requirement; configuration; procedure; environment; uncertainty; acceptance rule.	Test article; equipment; raw data; result; anomaly and disposition.
Process execution	Route revision; operation; performer; date/time; equipment; parameters; material; result.	Lot/serial; qualified procedure; inspection; nonconformity; next authorized step.
Change	ID; reason; baseline before/after; impact; approvals; effectivity; verification.	Affected requirements/items; delivered population; suppliers; support information.
Hazard or risk	ID; scenario; consequence; likelihood basis; exposure; controls; owner; residual decision.	Requirements; mitigations; verification evidence; operational limitations.
Release	ID; configuration; scope; acceptance evidence; concessions; restrictions; authorized identity; date.	Requirements baseline; product serial/lot; delivery dossier; service-life status.
Digital artifact	Artifact ID; version; source/build; dependencies; hash; signature; provenance; access class.	Requirements; verification; release; deployment instances; vulnerabilities.
Retirement	Asset identity; condition; hazardous inventory; reuse restrictions; disposition; verifier.	Life history; disposal evidence; retained records; remaining obligations.

Table D-2 — Filled illustrative trace chain

Source p. 55, 56 | Illustrative or explanatory source table

Record	Example value	Connection
Need	NEED-GSC-01: controlled motion during payload handling.	Allocated to SYS-GSC-R12.
Requirement	SYS-GSC-R12 rev B: stop response within a program-defined limit under stated load and speed.	Hazard H-GSC-02; verification V-GSC-12.
Configuration	Controller CTRL-07 rev C; firmware 2.4.1; cart serial GSC-004.	Build manifest BM-241; interface ICD-09 rev D.

Record	Example value	Connection
Verification	V-GSC-12 rev 3; test article GSC-004; report TR-012.	Raw records RAW-012; calibrated timer TM-08; approved decision rule DR-03.
Disposition	Anomaly AN-04 closed after independent retest.	NCR-026; verified corrective action CA-026.
Release	REL-GSC-004 rev 1; approved operating- domain restriction attached.	Release authority RA-02; receiving acknowledgement ACK-004.

Table O-1 — Required security and integrity records

Source p. 77 | Required structure when applicable

Record	Minimum content
Asset/trust model	Assets, identities, interfaces, zones, data flows, dependencies and trust assumptions.
Threat and impact assessment	Credible threats, exposure, safety/mission consequences, controls and residual decisions.
Access record	Role, identity, privileges, approver, start/end, emergency use and periodic review.
SBOM and dependencies	Components, versions, provenance, known exposure, support status and disposition.
Vulnerability record	Report source, affected versions, severity basis, exploitability context, mitigation, deadline and verification.
Update manifest	Target identity, old/new configuration, origin/integrity evidence, compatibility, authorization and rollback conditions.
Incident record	Timeline, evidence preservation, affected population, containment, communication, root cause and recovery approval.
Recovery test	RTO/RPO basis, backup identity, restoration duration, integrity checks, configuration reconciliation and result.
Crypto-agility record	Algorithms, keys/certificates, support horizon, dependencies, migration needs and verification.
Supplier interface	Access conditions, notification duties, update responsibilities, evidence rights and termination controls.

Table AJ-1 — Operational form set and mandatory payload

Source p. 128 | Required structure when applicable

Form ID / purpose	Required form-specific fields beyond AJ.1	Approval and control
F01 — Application and scope	Route; legal/holder identity; sites and remote functions; product/service/process/role identity; lifecycle responsibility; criticality; exclusions; actual operator authorization; evaluation access.	Applicant acknowledgement and independent application review before evaluation.
F02 — Application profile	Intended use/domain; requirements and limits; essential controls; methods; conditions; samples; uncertainty/scoring; acceptance rule; failure criteria; surveillance; changes; technical owners.	Competent technical approval before evaluating results.

Form ID / purpose	Required form-specific fields beyond AJ.1	Approval and control
F03 — Competence and assignment	Role; verified prerequisites; experience; training; examination/practical results; essential steps; witnessed work; authorized scope; conflicts; development; expiry and restrictions.	Competence approval separate from mere training delivery; assignment check before each job.
F04 — Audit or evaluation plan	Objectives; route; scope; criteria; sites/shifts; methods; team coverage; time calculation; sample design; access/security; meetings; reporting; technical witnessing.	Authorized plan review; actual departures and resulting coverage recorded.
F05 — Technical result and decision rule	Object/configuration; characteristic; specification; method; equipment; corrections; raw result; uncertainty/coverage; selected rule; result; limitations; technical disposition.	Competent technical sign-off; independent review for triggered criticality.
F06 — Nonconformity and corrective action	Exact requirement; evidence and gap; grade; affected population; protection; notification; occurrence/escape causes; actions; owners; original due dates; effectiveness; verified closure.	Finding classification, technical disposition and final closure separately attributable.
F07 — Review and attestation decision	Complete scope/profile; evaluation package; competence and independence; findings/closure; evidence limitations; decision and rationale; dates; issuer; required scope restrictions.	Independent reviewer/decision maker; no evaluator deciding own third-party evaluation.
F08 — Surveillance and status	Attestation ID; current scope; criticality; due dates; completed activities; findings; change triggers; status; restrictions; restoration/withdrawal; registry update.	Actual decision dates; no hidden gaps or deadline resets.
F09 — Supplier flow-down and transfer	Actual performer and sub-tiers; work package; essential instructions; acknowledgements; source approval; change notice; verification; custody; escape response; records and exit.	Commissioning organization retains acceptance and oversight accountability.
F10 — Personnel credential and task authority	Person; profile; knowledge/practical/essential results; independent decision; credential limits; employer task; site/equipment; supervision; practice; reassessment; expiry.	Separate credential and employer authorization decisions and status.
F11 — Complaint or appeal	Reporter/party; object; issue/grounds; dates; admissibility; conflicts; independent reviewer; submissions; evidence; interim measures; outcome; communication; corrective effects.	Independent outcome; protective action remains effective during review.
F12 — CAB competence scope	Legal provider; activity; method families; ranges/conditions; uncertainty capability where relevant; sites; competence; witnessing; findings; independent authority; exact authorized claim.	Actual competence decision; no self-accreditation or automatic equivalence.

Table AJ-2 — Cross-object record relationships

Source p. 129 | Required structure when applicable

Relationship	Required consistency check
F01 scope → F02 profile	Every claimed object and site is covered by a valid profile and applicable requirements; excluded responsibility is justified.
F03 competence → F04 plan	Assigned evaluators cover routes, sector, criticality, methods and language; conflicts are cleared.
F04 plan → F05 results	Actual objects, sites, methods, samples and configurations match the plan or an approved recorded deviation.

Relationship	Required consistency check
F05 result → F06 finding	Failed or indeterminate criteria are correctly reflected; no favorable score suppresses a critical gap.
F06 closure → F07 decision	Initial/renewal/extension decisions contain no open nonconformity in their scope; effectiveness is verified.
F07 decision → F08 status	The exact scope, dates, restrictions and ongoing/instance basis agree; no claim is broader than its decision.
F09 outsourced work → product/service dossier	Actual performer, source changes, lot identity and evidence reach the final delivered object.
F10 credential → employer task	Credential competence supports, but does not replace, the specific employer authorization.
F11 case → F07/F08 revisions	Appeal or complaint effects change only supported decisions/status and preserve their original history.
F12 body scope → issued reports	Each claimed accredited/authorized activity remains within the actual assessed technical scope.

Table AJ-3 — F02 profile example — AP-GSI-01, revision 1

Source p. 129 | Illustrative or explanatory source table

Field	Filled illustrative record
Route and object	SVC; dimensional inspection service for identified support-equipment parts; one evaluated site and controlled measuring station.
Domain and responsibility	Room-temperature dimensional inspection; no claim for destructive tests, complete vehicle safety or statutory approval.
Criterion	Characteristic EX-D01: 50.000 ± 0.030 mm for the fictional demonstration part; traceable actual-result report required.
Method and evidence	Approved procedure MP-01; corrected result; instrument identity; valid calibration; environmental record; uncertainty budget; actual raw observations.
Criticality and rule	C2 for this demonstration use; DR-A full-interval rule; uncertainty factor and basis recorded.
Release and failure	A competent authorized person signs the result. Missing configuration or an indeterminate critical result holds acceptance.
Continuing controls	C2 ongoing service surveillance no later than six months; method/site/critical equipment changes trigger review.
Claim limit	Only the described inspection service and method; no automatic product approval or laboratory accreditation.

Table AJ-4 — F04-F08 combined example — EVAL-EX-026

Source p. 130 | Illustrative or explanatory source table

Record stage	Filled illustrative record
Application	ORG; fictional support-equipment manufacturer; 80 effective personnel; one site; C2; special processes and assured digital acceptance.
Plan	B = 5; K = 1.35; f = 0.30; T = 9.0 auditor-days; readiness 2.5 and implementation 6.5; qualified specialists assigned; independent review separate.

Record stage	Filled illustrative record
Observed finding	NCR-EX-11: post-maintenance reference verification not enforced. Requirement 7.6/7.7; actual affected work and evidence recorded. Major classification based on control breakdown.
Protection	Affected measurements held; relevant earlier output traced; safe disposition and required notifications completed.
Correction and cause	Reference verified; occurrence and escape causes demonstrated; workflow amended and challenged under representative conditions.
Closure	Competent reviewer verifies implementation and effectiveness. No open nonconformity remains in the proposed ORG scope.
Decision	Independent decision maker grants only the evaluated ORG scope on the actual recorded decision date. Product and personnel routes not included.
Continuing status	Maximum ongoing validity 24 months; first C2 surveillance no later than six months; exact dates calculated from actual decision and recorded.

Table AJ-5 — F09-F10 bounded records

Source p. 130 | Illustrative or explanatory source table

Record	Filled illustrative content and decision
PER-EX-017 competence	Knowledge 86%; practical 92%; failed essential hold step. Initial decision refused. After successful documented remediation and equivalent practical reassessment, independent decision limited to the assessed dimensional-inspection role.
Employer task authorization TA-EX-17	Applies only after competence is demonstrated; approved measuring station and stated part family; current method and supervision limits; review no later than 12 months; C2 inactivity over six months requires observed demonstration.
Supplier approval SUP-EX-042	New bonded-assembly site proposed; existing corporate documentation does not prove site capability. Conditional development status permits controlled qualification trials only; production release held.
Source closure	Site-specific process qualification, operator authorization, environmental controls and representative first article verified. Approval record updated only for the demonstrated site and process window.
Sub-tier trace	Surface source S-10A and test laboratory L-07 approved for actual work; their evidence connects material M-31 and run BR-116 to the delivered bracket serial population.

Table AJ-6 — Controlling rules and common misinterpretations

Source p. 130, 131 | Required structure when applicable

Subject	Controlling provisions	Required interpretation
Scope and object	1.3; 2.2; Annexes A and AA	Activity triggers and retained responsibility determine requirements. PER applicants do not inherit corporate QMS obligations.
Criticality and independence	Annex B; 5.3; 9.6; Annex AB	Criticality drives technical assurance. Third-party decision independence is additional, not replaced by low criticality.

Subject	Controlling provisions	Required interpretation
Measurement decisions	7.7; Annex AD; informative Annex H	The pre-agreed normative decision rule controls; example numbers are not universal limits.
Product / service / process release	8.6; 23-25; Annexes C, K- M and AD	Qualification, routine release and independent certification are separate. Conditional progression is not conditional certification.
Auditor and personnel competence	7.2; 26; Annexes AB and AE	Knowledge scores, practical scores and all essential steps are separate pass conditions. Employer authorization remains distinct.
Subcontracted work	8.4; 27; Annexes J and AF	Requirements reach the actual performer; outsourcing does not remove retained accountability.
Audit time and frequency	Annexes AC and AG	AC controls resource floors and coverage; AG controls intervals. A smaller fee does not justify less evidence.
Findings and status	22; Annexes AD and AG	No open nonconformity at initial grant/renewal/extension. Existing minor continuation is bounded and documented.
Provider competence / accreditation	28; Annex AH	Organizational conformity is not accreditation; actual independent technical competence and authorization are required.
Appeals and protection	22.7; Annex AI	Fair independent review does not automatically suspend protective action or extend validity.
Edition and amendment	2.5; Annex Y	First Edition identifies the document. Amendments and recognition arrangements require their own actual controlled decisions.
Examples and calculations	0.5; Annexes E-I, U and Z	Synthetic values support methods; they do not establish the performance of an actual product or operation.

Appendix B — Local implementation and release

Readiness condition	Evidence before consequential use
Authority and responsibility	Actual legal operator, owner, competent technical authority, independent reviewer and permitted result class are recorded.
Scope and criteria	Object, configuration, site, period, trigger, every technical value or observable attribute, units and prospective approval are complete.
Evidence and methods	Original accessible evidence, representative observations, valid methods, uncertainty, adverse cases and limitations support the intended conclusion.
People and independence	Competence is current for each task; genuine conflicts, relevant prior work and needed separation have been checked.
Records and tools	Field meanings, unique IDs, original history, access, retention, recovery and actual deployed workflows have passed local validation.
Decision and public use	All relevant blockers are resolved; required independent decision and written permissions precede the exact public claim.
Continuity and handover	Receiving custody, unresolved duties, corrections and historical decisions survive transfer, retirement or provider closure.

Record the completed local readiness and actual authorization in AF-FR-9100-032 or an equivalent controlled record. Preserve the unchanged source standard and each earlier decision basis. A blocked activity may continue only within a genuinely permitted development boundary, not as a provisional conformity certificate.