



AF 9100:2026

Aerospace Quality Management System

PROCEDURE

Technical Tools, Data Integrity and Evidence Portability

AF-PR-9100-010

FIRST EDITION

30 September 2026 | English master text

Publication identity and application

Control	Publication value
Title	Technical Tools, Data Integrity and Evidence Portability
Document code	AF-PR-9100-010
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	Information assurance and tool owner
Primary source anchors	7.9, 7.11, 7.12, D, AJ.2, AJ.7
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 Trigger, inputs and handover	4
3 Operating sequence	4
4 Decision, interruption and escalation	5
5 Required records and receiving checks	5
6 Worked case and adverse challenge	5
Appendix A — Controlling source and evidence	7
Source tables — complete field and decision payloads	9
Appendix B — Local implementation and release	11
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 Trigger, inputs and handover

Trigger: A computational tool, data interface or repository is introduced, changed, recovered or retired.

Accountable process owner: Information assurance and tool owner. Actual named appointments and deputies are maintained locally.

Input to verify	Required output / receiving function
Exact request, object and source profile	Accepted scope and controlled work package, or a reasoned hold/refusal.
Current people, authority, data and equipment	Authorized assignment and evidence-access boundary.
Original execution, adverse evidence and source history	Attributable result, identified limitations and required action.
Relevant source clocks and actual event times	Genuine due/completion history and timely recipient communication.

3 Operating sequence

3.1 Define intended reliance

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

3.2 Control the baseline

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

3.3 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.

3.4 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.

3.5 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.

3.6 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.

4 Decision, interruption and escalation

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

State or event	Action and limit
Evidence valid and criteria met	Record the bounded result and pass it to the authorized receiving function; do not enlarge scope.
Evidence missing, invalid or inconclusive	Keep the dependent conclusion not yet demonstrated / HOLD, preserve the reason and define competent next work.
Valid evidence demonstrates failure	Record nonconformity and protect the affected population; follow actual technical disposition and source status controls.
Trigger genuinely absent	Record the exclusion and its approved responsibility basis. Resource shortages do not justify N/A.
Interrupted or changed work	Preserve prior state and actual configuration; complete impact and revalidation before claiming completion.

5 Required records and receiving checks

Document	Record purpose
AF-FR-9100-019	Software, AI, Model and Technical-Tool Release
AF-FR-9100-029	Cyber Incident, Update and Assured Recovery
AF-FR-9100-032	Publication, Adoption, Authority and Controlled Closure

At handover the receiver checks object, scope, current version, original evidence, open conditions, true event chronology and the action they may authorize. An email sent, field marked complete or invoice paid is not acceptance of that handover.

6 Worked case and adverse challenge

Synthetic scenario: A migration copies every file, but a test report links to the wrong serial.

Required reasoning: Reject semantic reconciliation despite matching file counts. Repair relationships, repeat the failing case and review conclusions already relying on the incorrect link.

Challenge before local use	Expected behavior
Missing essential input	Dependent conclusion remains held; no favorable default.
Wrong configuration or performer	Detect the mismatch and reassess relevant evidence.
Expired or conflicted authority	Block the prohibited assignment or decision; later renewal cannot validate earlier unauthorized work.
Failed mandatory condition with high total score	No compensation; preserve the failure and required action.

Challenge before local use	Expected behavior
Correction without original history	Reject an apparent closure that erases relevant earlier evidence.

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.

7.9 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.

7.11 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.

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.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 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.
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.

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.