



AF 9100:2026

Aerospace Quality Management System

TECHNICAL PROFILE BOOK

Cybersecurity, OT and Trusted Evidence — Technical Application Book

AF-TP-9100-003

FIRST EDITION

30 September 2026 | English master text

Publication identity and application

Control	Publication value
Title	Cybersecurity, OT and Trusted Evidence — Technical Application Book
Document code	AF-TP-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	Security and operational technology authority
Primary source anchors	13, O
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 Technical profile and prospective parameter completion	4
3 Subject-by-subject implementation	4
4 Representative evaluation and adverse evidence	6
5 Interface records, decisions and continuing use	6
Appendix A — Controlling source and evidence	7
Source tables — complete field and decision payloads	10
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

Defensive protection of products, connected processes and evidence; identity, dependency integrity, authorized testing, updates and semantic recovery.

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 Technical profile and prospective parameter completion

Trust boundary; privileged roles; approved connections; update target; security/safety conflicts; RTO/RPO; integrity checks; rollback restrictions

Parameter record	Content required before evaluating results
Identity and trigger	Stable criterion ID, source anchor, owner, actual object, phase, mode and reason it applies.
Limit or attribute	Value/range with compatible units and boundary convention, or an observable state with every essential step.
Technical basis	Actual environment, duty, consequence, derivation, qualified evidence and relevant approval.
Method and representation	Inspection, analysis, demonstration or test; method version, article/population, configuration and validity limits.
Uncertainty and decision	Corrections, model, covariance, coverage, pre-agreed rule, sample/scoring logic and hold conditions.
Authority and change	Technical and independent approvals, actual effectivity, preserved earlier basis and reopening triggers.

The fields above are completed for the actual application. A blank limit, undefined domain or unvalidated method prevents the dependent claim; the book deliberately does not invent one severity, tolerance or task threshold for unrelated applications.

3 Subject-by-subject implementation

13.1 — Security scope and integrated risk assessment

Source p. 31; complete conditions reproduced in Appendix A.

Implementation record: Asset and trust-boundary inventory; threat assessment; safety-security interface decisions.

Application check: 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.

Review boundary: Unknown target configuration, invalid evaluation or failed essential protection blocks consequential deployment. Record each source condition separately in the linked checklist and preserve approved exclusions.

13.2 — Identity, access and privileged actions

Source p. 31; complete conditions reproduced in Appendix A.

Implementation record: Access matrix; privileged approvals; identity lifecycle; emergency-access reviews.

Application check: 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.

Review boundary: Unknown target configuration, invalid evaluation or failed essential protection blocks consequential deployment. Record each source condition separately in the linked checklist and preserve approved exclusions.

13.3 — Secure development and supply-chain integrity

Source p. 31; complete conditions reproduced in Appendix A.

Implementation record: Secure-development plan; SBOM; dependency reviews; vulnerability decisions and mitigations.

Application check: 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.

Review boundary: Unknown target configuration, invalid evaluation or failed essential protection blocks consequential deployment. Record each source condition separately in the linked checklist and preserve approved exclusions.

13.4 — OT and connected-production safeguards

Source p. 31; complete conditions reproduced in Appendix A.

Implementation record: OT architecture; authorized connections; patch assessments; compensating controls; restoration tests.

Application check: 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.

Review boundary: Unknown target configuration, invalid evaluation or failed essential protection blocks consequential deployment. Record each source condition separately in the linked checklist and preserve approved exclusions.

13.5 — Secure updates, rollback and cryptographic agility

Source p. 31; complete conditions reproduced in Appendix A.

Implementation record: Update architecture; signed release manifest; interruption and rollback tests; cryptographic inventory and migration plan.

Application check: 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.

Review boundary: Unknown target configuration, invalid evaluation or failed essential protection blocks consequential deployment. Record each source condition separately in the linked checklist and preserve approved exclusions.

13.6 — Security testing and vulnerability handling

Source p. 31; complete conditions reproduced in Appendix A.

Implementation record: Authorized test plans; results; vulnerability register; remediation verification; customer communication.

Application check: 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.

Review boundary: Unknown target configuration, invalid evaluation or failed essential protection blocks consequential deployment. Record each source condition separately in the linked checklist and preserve approved exclusions.

13.7 — Incident response and recovery assurance

Source p. 32; complete conditions reproduced in Appendix A.

Implementation record: Incident plan; exercise records; RTO/RPO basis; integrity verification; return-to-service decision.

Application check: 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.

Review boundary: Availability restored without required integrity or protective evidence does not authorize assured use. Record each source condition separately in the linked checklist and preserve approved exclusions.

4 Representative evaluation and adverse evidence

Software, AI, Models and Trusted Updates

Witness or trace: Assess trust, privileges, vulnerabilities, OT compatibility and safety-security conflicts. Intrusive tests require written safe authorization; signatures alone do not establish technical suitability.

Synthetic challenge: A model's overall accuracy is high but a separately tested difficult defect set has low recall. Retain both populations and limitations. Resolve the critical domain or enforce a technically validated restriction; do not pool it into a favorable overall score.

Continuity, Emergency Interfaces and Assured Recovery

Witness or trace: Record real event chronology, affected configurations and outputs, original evidence and required notices. Keep protective operations distinct from investigation and public status administration.

Synthetic challenge: An exercise meets RTO 4 h and RPO 1 h but loses a configuration link. Record the time objectives as met and assured use as held. Correct and repeat the relationship check before accepting recovery.

Technical Tools, Data Integrity and Evidence Portability

Witness or trace: 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.

Synthetic challenge: A migration copies every file, but a test report links to the wrong serial. Reject semantic reconciliation despite matching file counts. Repair relationships, repeat the failing case and review conclusions already relying on the incorrect link.

5 Interface records, decisions and continuing use

Record	Required implementation purpose
AF-FR-9100-029	Cyber Incident, Update and Assured Recovery
AF-FR-9100-019	Software, AI, Model and Technical-Tool Release

Qualification, instance acceptance, current operating capability and independent attestation retain separate evidence and decisions. A new site, material, supplier, digital load, use environment or duty requires a relevant difference and requalification review. No previous result transfers automatically because the name is unchanged.

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.

13.1 Security scope and integrated risk assessment

SOURCE p. 31 | Normative when applicable

13.1(a) The organization shall identify digital assets, trust boundaries, dependencies, users and interfaces affecting assured outcomes. Threat scenarios shall be evaluated together with safety and mission consequences, including loss of integrity, availability, authenticity and confidentiality.

13.1(b) Security assumptions shall be reviewed across suppliers, remote services, maintenance access and physical access. The organization shall identify where a security measure could impair emergency operation or safety and resolve the conflict through a joint technical decision.

Required evidence: Asset and trust-boundary inventory; threat assessment; safety-security interface decisions.

13.2 Identity, access and privileged actions

SOURCE p. 31 | Normative when applicable

13.2(a) Access shall be based on verified identity, least necessary privilege and approved roles. Privileged access, remote maintenance and release-authority actions shall have strengthened authentication and traceable authorization appropriate to risk.

13.2(b) Access shall be removed or changed promptly when responsibilities end or change. Shared credentials shall not obscure accountability. Emergency access shall be controlled, logged, time-bounded and reviewed after use. Service accounts and machine identities shall be governed as well as human accounts.

Required evidence: Access matrix; privileged approvals; identity lifecycle; emergency-access reviews.

13.3 Secure development and supply-chain integrity

SOURCE p. 31 | Normative when applicable

13.3(a) Security requirements shall be integrated into development, procurement and maintenance. The organization shall assess dependency provenance, vulnerability exposure, secure configuration, supported versions and mechanisms for receiving security information.

13.3(b) A software bill of materials or equivalent controlled inventory shall identify relevant components and dependencies. Vulnerability disposition shall consider exploitability, exposure, safety consequences and available mitigations. Presence of a component in an inventory shall not itself demonstrate that it is secure.

Required evidence: Secure-development plan; SBOM; dependency reviews; vulnerability decisions and mitigations.

13.4 OT and connected-production safeguards

SOURCE p. 31 | Normative when applicable

13.4(a) Industrial networks and connected equipment shall be designed to limit unauthorized changes and propagation of failures. Appropriate segmentation, access control, backup, monitoring and safe degraded operation shall be established based on the process risk.

13.4(b) Patches, remote connections and security tools shall be evaluated for compatibility with timing, availability and safety. Where immediate patching is inappropriate, a time-bounded compensating-control decision shall be documented. Production data and machine-program integrity shall remain verifiable.

Required evidence: OT architecture; authorized connections; patch assessments; compensating controls; restoration tests.

13.5 Secure updates, rollback and cryptographic agility

SOURCE p. 31 | Normative when applicable

13.5(a) Updates shall verify origin, integrity, compatibility, authorization and intended target configuration before installation. The organization shall define interruption handling, recovery, anti-rollback needs and conditions for safe rollback without reintroducing an unacceptable vulnerability.

13.5(b) Cryptographic dependencies shall be inventoried and reviewed for supported algorithms, key management, certificate validity and migration capability. Future algorithm replacement shall be planned according to product life and threat exposure; this standard does not mandate a particular algorithm or claim universal post-quantum readiness.

Required evidence: Update architecture; signed release manifest; interruption and rollback tests; cryptographic inventory and migration plan.

13.6 Security testing and vulnerability handling

SOURCE p. 31 | Normative when applicable

13.6(a) Security testing shall have documented authorization, boundaries, safety precautions, data handling and restoration requirements. Methods shall be selected for the architecture and threat model. Test-induced operational or physical hazards shall be assessed before execution.

13.6(b) The organization shall provide a channel for vulnerability reports, assess credibility and impact, track remediation and communicate relevant actions to affected parties. Security findings shall remain connected to product configuration and safety assessment; closure shall require evidence, not only a changed status field.

Required evidence: Authorized test plans; results; vulnerability register; remediation verification; customer communication.

13.7 Incident response and recovery assurance

SOURCE p. 32 | Normative when applicable

13.7(a) The organization shall establish incident triage, containment, evidence preservation, technical escalation, communication and recovery responsibilities. Plans shall consider compromised engineering records, manufacturing programs, product updates and supplier credentials, not only office systems.

13.7(b) Recovery shall verify authenticity and consistency of restored data and configurations. A system shall not be returned to assured service solely because it is operational. Exercises shall demonstrate recovery time, recoverable data age and product-impact assessment under representative conditions.

Required evidence: Incident plan; exercise records; RTO/RPO basis; integrity verification; return-to-service decision.

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.

Source tables — complete field and decision payloads

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.

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.