



AF 9100:2026

Aerospace Quality Management System

CHECKLIST

Cybersecurity, OT and Trusted Evidence — Checklist

AF-CL-9100-004

FIRST EDITION

30 September 2026 | English master text

Publication identity and application

Control	Publication value
Title	Cybersecurity, OT and Trusted Evidence — Checklist
Document code	AF-CL-9100-004
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	Technical evaluator
Primary source anchors	13
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.

Interactive fields are blank by default. Save a working copy, use continuation records where necessary and preserve raw supporting evidence outside the PDF through controlled references. Separate issued PDFs are the authoritative interactive copies; the combined reading edition is flattened.

Contents and reading route

Publication identity and application	2
Contents and reading route	3
1 Checklist use and state definitions	4
2 Complete source-condition evaluation	5
4 Compound-condition continuation and final reconciliation	9

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 Checklist use and state definitions

Evaluate the whole source condition, including every joined sub-condition. Where different parts have different evidence, add separate continuation rows linked to the original identifier. Do not compress a compound requirement into a favorable summary.

Field state	Meaning
PASS	Conforming: valid evidence meets the approved applicable condition.
FAIL	Nonconforming: valid evidence demonstrates failure of the applicable requirement.
HOLD	Not yet demonstrated: applicability, criteria, evidence, validity, interpretation or authority remains unresolved.
N/A	Not applicable only with an approved absence-of-activity-and-responsibility rationale. Missing resources or access are not exclusions.

States in this companion map to the source’s requirement-status dictionary; operational record status and evidence validity remain separate. No prefilled state is supplied. A metric counts progress only and cannot override a mandatory failure.

Assessment / case / object / profile / evaluated version

Assessor / actual dates / route / sites / configuration / selected scope

Approved applicability and exclusions / continuation record location

2 Complete source-condition evaluation

13.1 — Security scope and integrated risk assessment

13.1(a) | Source p. 31

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.

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

STATE

EVIDENCE / APPROVED N/A BASIS

REVIEWER / ACTUAL EVENT

Gap / required action / continuation record:

13.1(b) | Source p. 31

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.

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

STATE

EVIDENCE / APPROVED N/A BASIS

REVIEWER / ACTUAL EVENT

Gap / required action / continuation record:

13.2 — Identity, access and privileged actions

13.2(a) | Source p. 31

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.

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

STATE

EVIDENCE / APPROVED N/A BASIS

REVIEWER / ACTUAL EVENT

Gap / required action / continuation record:

13.2(b) | Source p. 31

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.

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

STATE

EVIDENCE / APPROVED N/A BASIS

REVIEWER / ACTUAL EVENT

Gap / required action / continuation record:

13.3 — Secure development and supply-chain integrity

13.3(a) | Source p. 31

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.

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

STATE	EVIDENCE / APPROVED N/A BASIS	REVIEWER / ACTUAL EVENT

Gap / required action / continuation record:

13.3(b) | Source p. 31

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.

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

STATE	EVIDENCE / APPROVED N/A BASIS	REVIEWER / ACTUAL EVENT

Gap / required action / continuation record:

13.4 — OT and connected-production safeguards

13.4(a) | Source p. 31

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.

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

STATE	EVIDENCE / APPROVED N/A BASIS	REVIEWER / ACTUAL EVENT

Gap / required action / continuation record:

13.4(b) | Source p. 31

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.

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

STATE	EVIDENCE / APPROVED N/A BASIS	REVIEWER / ACTUAL EVENT

Gap / required action / continuation record:

13.5 — Secure updates, rollback and cryptographic agility

13.5(a) | Source p. 31

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.

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

STATE

EVIDENCE / APPROVED N/A BASIS

REVIEWER / ACTUAL EVENT

Gap / required action / continuation record:

13.5(b) | Source p. 31

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.

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

STATE

EVIDENCE / APPROVED N/A BASIS

REVIEWER / ACTUAL EVENT

Gap / required action / continuation record:

13.6 — Security testing and vulnerability handling

13.6(a) | Source p. 31

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.

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

STATE

EVIDENCE / APPROVED N/A BASIS

REVIEWER / ACTUAL EVENT

Gap / required action / continuation record:

13.6(b) | Source p. 31

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.

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

STATE

EVIDENCE / APPROVED N/A BASIS

REVIEWER / ACTUAL EVENT

Gap / required action / continuation record:

13.7 — Incident response and recovery assurance

13.7(a) | Source p. 32

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.

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

STATE	EVIDENCE / APPROVED N/A BASIS	REVIEWER / ACTUAL EVENT

Gap / required action / continuation record:

13.7(b) | Source p. 32

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.

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

STATE	EVIDENCE / APPROVED N/A BASIS	REVIEWER / ACTUAL EVENT

Gap / required action / continuation record:

4 Compound-condition continuation and final reconciliation

Duplicate these controlled continuation fields as needed. Each additional predicate retains its parent source identifier, object, criterion, evidence, actual result, gap and independent approval. The number of printed fields is not a limit on the required evidence.

Parent requirement / compound condition / applicable object

Separate criterion and approved technical basis

Method, actual configuration and original evidence

Result, uncertainty/rubric and PASS/FAIL/HOLD/N/A reason

Failed/held condition, owner, original due event and action

Approved exclusion and independent review reference

Final requirement population and unresolved conditions

Independent reviewer / decision authority / genuine approval reference

Initial grant, renewal and extension require closure of all in-scope nonconformities and the source's complete decision conditions. A separate authorized technical concession does not make a failed original criterion conforming. Preserve independent review, actual authority and precise scope.