



AF 9100:2026

Aerospace Quality Management System

PROCEDURE

Continuity, Emergency Interfaces and Assured Recovery

AF-PR-9100-026

FIRST EDITION

30 September 2026 | English master text

Publication identity and application

Control	Publication value
Title	Continuity, Emergency Interfaces and Assured Recovery
Document code	AF-PR-9100-026
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	Continuity owner and technical return authority
Primary source anchors	6.5, 13.7, 19.5, 24.6, 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 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	10
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: Loss of critical staff, supplier, utility, site, data service or protective support.

Accountable process owner: Continuity owner and technical return authority. 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 Identify dependencies and failure scenarios

Record critical functions, maximum tolerable interruptions under the real profile, recovery objectives, alternate sources and common failures.

3.2 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.

3.3 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.

3.4 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.

3.5 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.

3.6 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.

4 Decision, interruption and escalation

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

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-9100-029	Cyber Incident, Update and Assured Recovery
AF-FR-9100-017	Resources, Facility and Tool Commissioning
AF-FR-9100-006	Nonconformity, Containment and Corrective Action
AF-FR-9100-008	Surveillance, Renewal and Status

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: An exercise meets RTO 4 h and RPO 1 h but loses a configuration link.

Required reasoning: Record the time objectives as met and assured use as held. Correct and repeat the relationship check before accepting recovery.

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.

Challenge before local use	Expected behavior
Failed mandatory condition with high total score	No compensation; preserve the failure and required action.
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.

6.5 Resilience and continuity planning

SOURCE p. 17 | Normative when applicable

6.5(a) The organization shall identify critical dependencies such as energy, utilities, specialist personnel, sole-source materials, digital services, test infrastructure and transport. It shall assess credible disruptions, time to recover and the ability to continue meeting quality and safety obligations during degraded operation.

6.5(b) Continuity plans shall define recovery priorities, alternative sources, data restoration, communication and restart qualification. Exercises shall include loss of a critical supplier and compromise of technical records where relevant. Emergency capacity shall not be assumed capable until its configuration, competence and process controls are demonstrated.

Required evidence: Business-impact analysis; continuity plans; exercise results; approved recovery and restart evidence.

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.

19.5 Hazardous tests and emergency preparedness

SOURCE p. 38 | Normative when applicable

19.5(a) Tests involving hazardous energy shall have a documented safety review, approved boundaries, instrumentation, protective arrangements, personnel authorization and emergency response. Test acceptance criteria and safety-abort criteria shall be distinguished.

19.5(b) After a test anomaly or protective-system intervention, restart shall require an authorized assessment. The organization shall preserve data and inspect affected equipment or articles before reuse. Lessons shall be incorporated into subsequent test readiness.

Required evidence: Test safety review; readiness approval; abort rules; anomaly evidence; restart and reuse decisions.

24.6 Continuity, disruption and customer protection

SOURCE p. 44 | Normative when applicable

24.6(a) The provider shall define disruption triggers, prioritization, communication, safe degraded operation, restoration objectives and acceptance after recovery. Exercises shall test actual dependencies and personnel availability. Alternative delivery arrangements shall be qualified before being relied upon for critical work.

24.6(b) When an incident may have affected earlier service outputs, the provider shall trace and assess those outputs, notify affected recipients as required and correct consequential errors. Meeting restoration-time objectives shall not close an unresolved accuracy, safety or evidence-integrity issue.

Required evidence: Continuity plan; exercised recovery; qualified alternatives; affected-output analysis; customer notifications.

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.