



AF 9100:2026

Aerospace Quality Management System

POLICY

Quality, Safety and Mission Assurance Policy

AF-PL-9100-001

FIRST EDITION

30 September 2026 | English master text

Publication identity and application

Control	Publication value
Title	Quality, Safety and Mission Assurance Policy
Document code	AF-PL-9100-001
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	Accountable executive
Primary source anchors	5.1, 5.2, 5.5, 6.1, 11.5, B
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 Policy commitments and prohibited conduct	4
3 Responsibilities, implementation and review	5
4 Implementation instruments	5
Appendix A — Controlling source and evidence	6
Source tables — complete field and decision payloads	8
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 Policy commitments and prohibited conduct

2.1 Governance, Delegation, Impartiality and Stop Authority

The responsible function maintains governance, delegation, impartiality and stop authority within its actual scope. Unresolved conflicts, expired delegation or a failed essential protective control prevent the affected authorization.

Policy application: Identify the accountable executive, management representative and relevant design, safety, production, digital, metrology and release authorities. State scope, limits, substitutes and reporting paths in written appointments. Technical return requires evidence of cause, extent and restored controls. Scheme status and public claims are separate decisions. Examine attempted interference and act on independent dissent rather than closing it by management preference.

2.2 Risk, Criticality, Hazards and Residual Acceptance

The responsible function maintains risk, criticality, hazards and residual acceptance within its actual scope. Unsupported critical consequence, unverified protection or unacceptable residual risk prevents dependent progression.

Policy application: Identify the exact function, configuration, phase, environment, exposure and people or assets affected. Include storage, maintenance, foreseeable misuse and retirement as well as nominal operation. Connect anomalies, source changes, life extensions and new observations to the original hazard argument. Trace affected releases and notify owners; closure of an action is not proof that risk was reduced.

2.3 Design, Systems Engineering and Lifecycle Gates

The responsible function maintains design, systems engineering and lifecycle gates within its actual scope. Unresolved essential interface, unsafe residual condition or unsupported model use holds the dependent gate.

Policy application: Record users, success and protective states, environments, support assumptions and lifecycle roles. Allocate verifiable requirements to physical, digital, human and service functions. Reconcile qualification, anomalies, actual configuration, operating procedures, training and support. Conditional progression may permit bounded non-dependent work but not action relying on missing critical evidence.

2.4 Technical Acceptance, Reporting and Authorized Release

The responsible function maintains technical acceptance, reporting and authorized release within its actual scope. Unclosed release blocker, unsupported configuration or unavailable authority prevents release of the dependent claim.

Policy application: Record serial, lot, event or family configuration, actual scope and the approved requirement and decision basis. Separate internal release from independent conformity attestation. Preserve recipients, evidence and installed or delivered identity. Correct material reporting errors transparently and review affected releases after new information invalidates the basis.

3 Responsibilities, implementation and review

Function	Policy responsibility
Accountable executive	Provide resources, protect independence, approve policy application and respond to systemic adverse evidence.
Technical and process owners	Translate commitments into applicable controls, prospective criteria and genuine records.
Independent assurance	Challenge unsupported decisions and report unresolved threats through an uninvolved authority.
All relevant personnel	Use current instructions, report actual observations, preserve adverse evidence and stop unsupported consequential work.

Explain this policy in forms and language understood at the actual point of use. Evaluate application through decisions and records rather than attendance alone. Review after material change, serious concern and the applicable management review; do not invent an additional universal review calendar.

4 Implementation instruments

Procedure code	Operating instrument
AF-PR-9100-003	Governance, Delegation, Impartiality and Stop Authority
AF-PR-9100-004	Risk, Criticality, Hazards and Residual Acceptance
AF-PR-9100-012	Design, Systems Engineering and Lifecycle Gates
AF-PR-9100-020	Technical Acceptance, Reporting and Authorized Release

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.

5.1 Executive accountability and customer focus

SOURCE p. 15 | Normative when applicable

5.1(a) Top management shall be accountable for system effectiveness and shall integrate quality, safety, reliability and delivery obligations into business decisions. It shall provide resources, resolve cross-functional conflicts and require evidence that commitments can be fulfilled before they are accepted.

5.1(b) Top management shall ensure that customer and end-user needs, applicable obligations and foreseeable consequences are understood. Product conformity, on-time delivery, complaints, repeat escapes and effectiveness of corrective action shall be reviewed together. Delivery recovery shall not be achieved by concealing defects or bypassing release controls.

Required evidence: Executive reviews; resource decisions; commitment reviews; balanced performance measures and escalations.

5.2 Policy and measurable commitments

SOURCE p. 15 | Normative when applicable

5.2(a) The organization shall establish an approved quality and assurance policy appropriate to its scope and risks. The policy shall commit to fulfillment of applicable requirements, accurate evidence, ethical behavior, reporting of concerns and continual improvement. It shall provide a practical basis for objectives and decisions.

5.2(b) The policy shall be communicated in language and forms understood by personnel and relevant external providers. Understanding shall be evaluated through observed decisions and interviews rather than a signature alone. The current policy shall be available to relevant interested parties subject to legitimate information controls.

Required evidence: Approved policy; communication records; observed application; linked objectives.

5.5 Stop-work and release protection

SOURCE p. 16 | Normative when applicable

5.5(a) Every person performing work affecting conformity shall know how to stop or hold an unsafe or potentially nonconforming activity. Defined hold conditions shall include loss of configuration identity, unverified critical characteristics, suspect counterfeit material, compromised evidence and operation outside an approved safety envelope.

5.5(b) Restart or release shall require an authorized assessment of cause, extent, implemented controls and remaining obligations. Commercial management shall not override a technical hold without the required technical and, where applicable, customer or authority approval. The decision and evidence shall remain traceable.

Required evidence: Stop-work instruction; hold records; restart criteria and authorized decisions.

6.1 Risk planning and acceptance

SOURCE p. 16 | Normative when applicable

6.1(a) The organization shall identify adverse uncertainties that can affect conformity, safety, mission outcomes, integrity of evidence or continuity of supply. The method shall address organizational and operational risks, interfaces, common-cause effects and credible combinations of failures. Risk ownership and acceptance authority shall be explicit.

6.1(b) Risk evaluations shall identify consequence, likelihood basis, exposure, existing controls and uncertainty. Ordinal categories shall not be treated as precise probabilities. A high-severity hazard shall not be accepted solely because an unsubstantiated likelihood estimate or a multiplied score is low.

6.1(c) Controls shall be selected, implemented and verified; residual risk shall then be assessed against approved criteria. Decisions shall specify assumptions, limitations, monitoring and review triggers. Unresolved binding requirements and unacceptable residual risks shall prevent the relevant release or lifecycle transition.

Required evidence: Risk register; hazard analyses; acceptance criteria; control verification; residual-risk decisions and triggers.

11.5 Hazard analysis and assurance case

SOURCE p. 28 | Normative when applicable

11.5(a) The organization shall maintain a structured safety and mission-assurance argument proportionate to criticality. Claims shall be bounded by configuration and operational domain and supported by traceable evidence. The argument shall expose uncertainty, counter-evidence and unresolved limitations.

11.5(b) Hazard analysis shall be maintained as the design and operating context evolve. Failure-mode analysis, fault trees, scenario analysis and other methods shall be selected for the problem rather than used as paperwork substitutes. Shared resources, common software, environmental exposure and organizational dependencies shall be assessed.

Required evidence: Assurance case; hazard log; analysis rationale; evidence index; limitations and independent challenge.

B.1 Classification method

SOURCE p. 52 | Normative when applicable

B.1(a) The organization shall classify functions, items, processes and evidence-producing tools by the highest credible consequence of their failure within the defined context. It shall consider exposure, combinations, common causes, detectability, recovery and uncertainty. Classification shall not be based only on financial value or a single multiplied risk score.

B.1(b) The classification shall be reviewed by competent technical personnel and approved by the assigned acceptance authority. Where the consequence is uncertain, the organization shall use a conservative provisional category or obtain the missing evidence before lowering assurance. An external mandatory classification shall remain applicable independently.

Required evidence: Classification record; hazard link; assumptions; reviewers; approval and change rationale.

B.2 No averaging across critical failures

SOURCE p. 52 | Normative when applicable

B.2(a) A favorable average score shall not compensate for a missing critical control, failed mandatory criterion or unsupported residual-risk acceptance. The organization shall identify release-blocking conditions and apply them before considering aggregate maturity or performance measures.

B.2(b) Quantitative safety or reliability objectives shall be derived from the applicable mission and authority basis. This annex does not prescribe universal probability targets. Evidence requirements shall consider uncertainty and the capability of the selected method to support the claimed objective.

B.2(c) The C0-C3 category controls technical assurance and surveillance intensity; it does not relax the independent review and decision requirements for a third-party attestation in Annexes AA and AD.

B.3 Example classification decision

SOURCE p. 53 | Definition, explanation or informative example; no new universal limit

B.3(a) Illustrative case: a software-controlled ground-support cart can move an expensive payload while personnel work nearby. The initial assessment identifies credible severe crush injury if unintended motion occurs. The relevant motion-control function is provisionally C2, not C0 merely because the cart is a support device. A qualified assessment may determine a different category when actual exposure and safeguards are known.

B.3(b) The example decision requires independently reviewed motion limits, verified stop functions, configuration control, operator validation and a residual-risk decision. It does not assign a universal automotive safety- integrity level or establish a certified cart design.

Source tables — complete field and decision payloads

Table B-1 — AF consequence categories

Source p. 52 | Required structure when applicable

Category	Consequence basis	Minimum assurance response
C0 — Ordinary	No credible safety effect or significant mission/service consequence within the stated use.	Controlled requirements, competent execution, acceptance evidence and proportionate internal review.
C1 — Significant	Recoverable degradation, material rework or service interruption with no credible severe injury or comparable high-consequence effect.	Documented risk and interface review; verification plan; reviewer not the sole originator where practicable; defined recovery.
C2 — Critical	Credible serious injury, major mission loss, major environmental harm or prolonged loss of an essential service.	Formal hazard analysis; independent technical review; controlled critical characteristics; demonstrated mitigations; authorized residual- risk decision.
C3 — Catastrophic	Credible fatalities, catastrophic system loss with safety consequences, or comparable catastrophic harm in the applicable domain.	Organizationally independent assurance challenge; explicit safety case; rigorous evidence and configuration control; highest designated technical and accountable approvals.

Table B-2 — Tailoring dimensions

Source p. 52 | Required structure when applicable

Dimension	C0 / C1 baseline	C2 / C3 additional expectation
Requirements	Defined acceptance criteria and controlled changes.	Bidirectional traceability of safety/mission controls; independent review of derived requirements.
Design and evidence	Review appropriate to complexity.	Independent verification of critical assumptions and evidence; unresolved counter-evidence escalated.
Suppliers	Scope-based approval and monitoring.	Critical sub-tier visibility; process qualification; authenticity strategy; change and escape notification.
Measurement	Suitable method and equipment.	Uncertainty and decision risk explicitly justified for critical acceptance characteristics.
Software and AI	Controlled versions and functional verification.	Assurance independence, failure-domain analysis, robust anomaly control and bounded adaptation.

Dimension	C0 / C1 baseline	C2 / C3 additional expectation
Release	Authorized person confirms completed plan.	Critical-control completeness, safety review and independent challenge of remaining limitations.
Field support	Feedback and corrective action.	Population traceability, urgent notification, monitored safety assumptions and lifecycle support.
Change	Impact-based review.	Reopen affected safety arguments and qualification; approval at an equivalent authority level.

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.