



AF 9100:2026

Aerospace Quality Management System

PROCEDURE

Risk, Criticality, Hazards and Residual Acceptance

AF-PR-9100-004

FIRST EDITION

30 September 2026 | English master text

Publication identity and application

Control	Publication value
Title	Risk, Criticality, Hazards and Residual Acceptance
Document code	AF-PR-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	Safety or mission assurance authority
Primary source anchors	6.1, 8.1.1, 8.1.3, 11.5, B, E
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	10
Appendix B — Local implementation and release	13

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: New mission, product, process, activity, material change or newly credible adverse consequence.

Accountable process owner: Safety or mission assurance 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 Define the scenario

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.

3.2 Classify by consequence

Assign the highest credible C0-C3 consequence with assumptions and reviewer identity. Use a conservative provisional position when consequence is unresolved; cost or an ordinal product cannot replace a safety basis.

3.3 Analyze mechanisms and dependencies

Choose methods that reveal initiating events, local and system effects, common causes, detection and failed interfaces. State probabilities only with compatible populations, exposure and supported models.

3.4 Allocate and verify protection

Convert each relied-upon mitigation into a controlled requirement with an owner, acceptance condition and verification. Examine whether a human action has enough time and information to work.

3.5 Decide residual risk

Record remaining uncertainty, counter-evidence, restrictions and authorized acceptance at the required independence level. An unresolved mandatory condition cannot be waived by calling it accepted risk.

3.6 Reopen when the basis changes

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.

4 Decision, interruption and escalation

Unsupported critical consequence, unverified protection or unacceptable residual risk prevents dependent progression.

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-9100-014	Risk, Hazard, Criticality and Residual Decision
AF-FR-9100-016	Design, Interfaces, Gates and Engineering Budgets
AF-FR-9100-006	Nonconformity, Containment and Corrective Action

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 expensive support cart is classified C0 because it is not flight hardware.

Required reasoning: Reassess actual human exposure and credible unintended movement. Use consequence rather than equipment label; require the corresponding technical review and protective evidence.

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.

6.1 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.

8.1.1 Operational risk management

SOURCE p. 20 | Normative when applicable

8.1.1(a) For each program, order or family of work, the organization shall identify operational risks to requirements, delivery and lifecycle outcomes. The assessment shall cover new technology, difficult characteristics, supplier capability, work transfers, maintenance constraints and changes in the intended environment.

8.1.1(b) The organization shall establish risk criteria, ownership, mitigation actions and residual-risk approval before the relevant gate. Risk records shall be updated when test evidence, nonconformities or field experience change the likelihood or consequence basis. A closed mitigation action shall be distinguished from demonstrated risk reduction.

Required evidence: Program risk register; mitigation verification; residual-risk acceptance; changes based on new evidence.

8.1.3 Product safety and mission-critical controls

SOURCE p. 20 | Normative when applicable

8.1.3(a) The organization shall identify product and service hazards throughout the lifecycle, including interfaces, foreseeable misuse, maintenance, transport, abnormal modes and retirement. Safety responsibilities shall extend to suppliers and field support within the organization's scope.

8.1.3(b) Safety-critical items and functions shall have explicit controls, acceptance criteria, independent review and traceability to hazard mitigations. Changes, concessions and nonconformities affecting these controls shall receive safety impact assessment before disposition. A generic quality approval shall not substitute for the required safety decision.

8.1.3(c) The organization shall provide relevant safety information to users, maintainers and downstream organizations, monitor safety-related events and support timely corrective action. Safety concerns shall be escalated even when the contractual acceptance criteria appear to have been met.

Required evidence: Hazard log; safety-control traceability; independent reviews; safety communications; in-service event assessments.

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.

E.1 Choosing an analysis method

SOURCE p. 57 | Definition, explanation or informative example; no new universal limit

E.1(a) A useful assessment begins with the decision and the system boundary. Process FMEA is appropriate for examining operation-level failure and escape mechanisms; design FMEA helps examine component or function failures; fault trees examine combinations contributing to an event; scenario analysis addresses interactions and unusual operating states. None is automatically sufficient for every system.

E.1(b) The analysis should record credible failure modes, initiating conditions, local and system effects, exposed populations, detection, mitigation, evidence and ownership. The analyst should actively seek shared dependencies and conditions that can defeat multiple safeguards. Negative evidence, uncertainty and model limitations should remain visible.

E.2 Severity-first FMEA interpretation

SOURCE p. 57 | Definition, explanation or informative example; no new universal limit

E.2(a) A priority index may help organize work, but multiplying ordinal severity, occurrence and detection scores does not create a physical risk quantity. Two rows with the same product can represent very different consequences. A serious hazard with uncertain occurrence should remain visible even when its numerical ranking is lower than a frequent cosmetic defect.

E.2(b) For example, an illustrative severity score of 10 with occurrence 1 and detection 2 produces 20, while a cosmetic issue with scores 2, 8 and 8 produces 128. The larger product does not make the cosmetic issue more safety-critical. A sensible response uses severity gates, evidence quality and explicit critical-control decisions in addition to prioritization.

E.3 Probability calculations and dependence

SOURCE p. 58 | Definition, explanation or informative example; no new universal limit

E.3(a) Consider two synthetic failure events with probabilities $P(A)=0.002$ and $P(B)=0.003$ over the same defined exposure. Under independence, the probability of either event is $1-(1-0.002)(1-0.003)=0.004994$. The probability of both is $0.002 \times 0.003 = 0.000006$. These calculations are conditional on the stated model, not measured performance.

E.3(b) Without independence, $P(A \text{ and } B)$ cannot be obtained by multiplication. The general union relation is $P(A \text{ or } B) = P(A) + P(B) - P(A \text{ and } B)$. From the given marginals alone, the intersection lies between 0 and 0.002; the union lies between 0.003 and 0.005. Shared power, common software or environmental exposure can invalidate the independent model.

Source calculation note: (E-1) $P(A \cup B) = P(A) + P(B) - P(A \cap B)$ All probabilities must refer to the same population and exposure. The equation is an identity; the independent-product approximation is an additional assumption, not part of the identity.

E.4 Common-cause sensitivity example

SOURCE p. 58 | Definition, explanation or informative example; no new universal limit

E.4(a) Assume, purely for illustration, a common-cause event has probability $q=0.001$ and causes both channels to fail. Conditional on no common cause, the channel failure probabilities are 0.002 and 0.003 and are independent. The combined loss probability is $q + (1-q) \times 0.002 \times 0.003 = 0.001005994$, much larger than 0.000006.

E.4(b) This is a sensitivity demonstration, not a validated common-cause model. It shows why a redundancy claim needs evidence about independence, common environments, implementation diversity and shared resources. A reviewer should challenge an analysis whose impressive result comes mainly from assuming every dependency away.

E.5 Risk acceptance record and review

SOURCE p. 58 | Definition, explanation or informative example; no new universal limit

E.5(a) A defensible record states the scenario, configuration, applicable obligations, controls, evidence, uncertainty, residual risk, decision authority, operating restrictions and review trigger. Acceptance should be withdrawn or reconsidered when an assumption is violated or material counter-evidence appears.

E.5(b) The record should distinguish a technical decision from an administrative acknowledgement. "Customer informed" is not the same as "customer authorized the specific departure", and neither can waive an applicable authority requirement. Acceptance should not be retroactively inferred from use of the product.

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.

Table E-1 — Minimum useful hazard-log content

Source p. 57 | Illustrative or explanatory source table

Record element	Purpose and example
Identity and configuration	H-GSC-02; ground-support cart GSC-004; configuration baseline CB-03.
Scenario and phase	Unintended movement during payload handling while personnel are in the access zone.
Initiating conditions	Incorrect command, stale state information, control failure or maintenance misconfiguration.
Consequences and exposure	Potential personnel injury and payload damage; exposure depends on task and exclusion-zone effectiveness.
Existing controls	Physical access control, motion authorization, stop function, operator procedure; each linked to a requirement.
Likelihood basis	Relevant field data or analysis with conditions and uncertainty; “unlikely” without evidence is not a quantitative estimate.
Verification and evidence	Test case, representative load, software version, independent review and anomaly disposition.
Residual decision	Named authority; accepted operating boundary; unresolved limitations; monitoring and review date.
Change triggers	Software, payload, speed, terrain, access zone, operator procedure or failure evidence changes.

Table E-2 — Filled illustrative FMEA extract

Source p. 57 | Illustrative or explanatory source table

Failure / effect	Occurrence control	Escape control and evidence	Decision
Incorrect controller version / motion behavior differs from validated baseline.	Signed release manifest and controlled installation; prevent unauthorized update.	Read-back version/hash and functional verification at deployment.	Hold release until identity is reconciled; review actual installed population.
Measurement bias / nonconforming dimension accepted.	Calibration, temperature control and validated method.	Uncertainty-aware decision rule; independent check of affected interval.	Assess prior accepted output; recalibration alone does not close the event.

Failure / effect	Occurrence control	Escape control and evidence	Decision
Supplier material substitution / hidden strength or environmental mismatch.	Approved source and change notification; controlled specification.	Identity and certificate validation plus risk-based confirmatory testing.	Obtain design-authority disposition; no automatic equivalence.
Scratched non-functional label / reduced readability.	Handling improvements and suitable label material.	Visual criterion and readability check.	Correct according to actual function; escalate if identification or warnings are impaired.

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.